Admin OUTPUT.txt

acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
------------------------------------------
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
------------------------------------------
aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install

Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
------------------------------------------
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.

Software\SmartLine Vision\aports not found.

------------------------------------------
appcompatflags v.20130930
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.

Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted
    C:\ProgramData\WebEx\WebEx\1524\atinst.exe
    C:\Users\Abe-Arjun.Mallik\Desktop\flashplayer19ax_ce_install.exe
    C:\Users\Abe-Arjun.Mallik\Downloads\Firefox Setup Stub 41.0.2.exe
    C:\Users\Abe-Arjun.Mallik\Downloads\flashplayer19_ce_install.exe
------------------------------------------
applets v.20140723
(NTUSER.DAT) Gets contents of user's Applets key

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Tue Apr 19 20:03:27 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
------------------------------------------
Software\Microsoft\IntelliPoint\AppSpecific not found.
------------------------------------------
Software\Ares not found.
------------------------------------------
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
------------------------------------------
autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task

Control Panel\Desktop

AutoEndTasks value not found.
------------------------------------------
autorun v.20081212
(NTUSER.DAT) Gets autorun settings

NoDriveTypeAutoRun    0xff
HonorAutorunSetting not found.

Page 1

Dell

Admin OUTPUT.txt

Autorun settings in the HKLM hive take precedence over those in
the HKCU hive.
----------------------------------------
bitbucket_user v.20091020
(NTUSER.DAT) TEST - Get user BitBucket values

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Wed Apr 20 12:57:38 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume
LastWrite Time = Wed Apr 20 12:57:38 2016 (UTC)


----------------------------------------
brisv v.20130429
(NTUSER.DAT) Detect artifacts of a Troj.Brisv.A infection

Software\Microsoft\PIMSRV not found.
----------------------------------------
cain v.20110204
(NTUSER.DAT) Extracts details for Cain & Abel by oxid.it

Software\Cain\Settings not found.

----------------------------------------
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.

----------------------------------------
clampi v.20091019
(NTUSER.DAT) TEST - Checks for keys set by Trojan.Clampi PROT module

Software\Microsoft\Internet Explorer\Main
LastWrite Time Wed Apr 20 16:55:00 2016 (UTC)

        Use FormSuggest = no

Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)

        AutoSuggest = yes

Software\Microsoft\Internet Account Manager\Accounts not found.

The system does not appear to have been infected with the Trojan.Clampi
PROT module.
----------------------------------------
clampitm v.20100624
(NTUSER.DAT) Checks for IOCs for Clampi (per Trend Micro)

ClampiTM plugin
Software\Microsoft\Internet Explorer\Settings
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

No Clampi values found.
----------------------------------------
comdlg32 v.20121008

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time Wed Apr 20 13:24:11 2016 (UTC)
CIDSizeMRU

Page 2

Admin OUTPUT.txt
LastWrite: Wed Apr 20 15:48:24 2016
Note: All value names are listed in MRUListEx order.

   firefox.exe
   rundll32.exe
   {003F09F1-A614-4993-A6EF-D5FAF3344DBF}

LastVisitedPidlMRU
LastWrite: Wed Apr 20 15:48:24 2016
Note: All value names are listed in MRUListEx order.

   firefox.exe - My Computer\C:\Users\Abe-Arjun.Mallik\Documents\Misc\Downloads
   {003F09F1-A614-4993-A6EF-D5FAF3344DBF} - Libraries

OpenSavePidlMRU
LastWrite: Wed Apr 20 13:24:11 2016
OpenSavePidlMRU\*
LastWrite Time: Wed Apr 20 13:24:11 2016
Note: All value names are listed in MRUListEx order.

   Libraries

OpenSavePidlMRU\docx
LastWrite Time: Wed Apr 20 13:24:11 2016
Note: All value names are listed in MRUListEx order.

   Libraries


-----------------------------------------------
compatassist
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)
   C:\ProgramData\WebEx\WebEx\1524\atinst.exe
   C:\Users\Abe-Arjun.Mallik\Desktop\flashplayer19ax_ce_install.exe
   C:\Users\Abe-Arjun.Mallik\Downloads\Firefox Setup Stub 41.0.2.exe
   C:\Users\Abe-Arjun.Mallik\Downloads\flashplayer19_ce_install.exe
-----------------------------------------------
compdesc v.20080324
(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions not found.
-----------------------------------------------
controlpanel v.20080428
(NTUSER.DAT) Look for RecentTask* values in ControlPanel key (Vista)

Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel
LastWrite Time Tue Apr 19 20:03:26 2016 (UTC)

Analysis Tip: The RecentTask* entries appear to only be populated through the
choices in the Control Panel Home view (in Vista). As each new choice is
selected, the most recent choice is added as RecentTask1, and each
RecentTask* entry is incremented and pushed down in the stack.

AllItemsIconView 1
StartupPage     1

-----------------------------------------------
cpldontload v.20100116
(NTUSER.DAT) Gets contents of user's Control Panel don't load key

Control Panel\don't load

Admin OUTPUT.txt
LastWrite Time Wed Apr 20 12:57:47 2016 (UTC)

Control Panel\don't load has no values.
------------------------------------------
decaf v.20110210
(NTUSER.DAT) Extracts the EULA value for DECAF.

Software\DECAFme not found.

------------------------------------------
dependency_walker v.20110204
(NTUSER.DAT) Extracts Recent File List for Dependency Walker.

Software\Microsoft\Dependency Walker\Recent File List not found.

------------------------------------------
domains v.20100116
(NTUSER.DAT) Gets contents Internet Settings\ZoneMap\Domains key

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)

cberedrweb [Tue Apr 19 20:03:24 2016 (UTC)]
   * -> 1

fda.gov [Tue Apr 19 20:03:24 2016 (UTC)]
   * -> 1

hhs.gov [Tue Apr 19 20:03:24 2016 (UTC)]

------------------------------------------
environment v.20110204
(NTUSER.DAT) Extracts user's Environment paths from NTUSER.DAT

Environment
Environment
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

TEMP -> %USERPROFILE%\AppData\Local\Temp
TMP -> %USERPROFILE%\AppData\Local\Temp

------------------------------------------
fileexts v.20080818
(NTUSER.DAT) Get user FileExts values

fileexts
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

------------------------------------------
filehistory v.20120620
(NTUSER.DAT) Gets filehistory settings

Software\Microsoft\Windows\CurrentVersion\FileHistory not found.
------------------------------------------
gthist v.20100218
(NTUSER.DAT) Gets Google Toolbar Search History

Software\Google\NavClient\1.1\History not found.
------------------------------------------
gtwhitelist v.20100218
(NTUSER.DAT) Gets Google Toolbar whitelist values

Software\Google\Google Toolbar\4.0\whitelist not found.

Page 4

Admin OUTPUT.txt
------------------------------------------
haven_and_hearth v.20110204
(NTUSER.DAT) Extracts the username and savedtoken for Haven & Hearth.

Software\JavaSoft\Prefs\haven not found.


------------------------------------------
ie_settings v.20130731
(NTUSER.DAT) Gets important user IE settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)

User Agent = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade = Wed Apr 20 12:57:37 2016 (UTC)
DaysToKeep = 40

Software\Microsoft\Internet Explorer\Main\WindowsSearch
LastWrite Time Wed Apr 20 16:55:46 2016 (UTC)
Version = 6.1.7601.17610

'Cleared' value not found.

LastCrawl = Wed Apr 20 16:55:46 2016 UTC
UpgradeTime = Wed Apr 20 16:54:59 2016 UTC
User Favorites Path = file:///C:\Users\Abe-Arjun.Mallik\Favorites\
------------------------------------------
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
  Download Directory = 'C:\Users\Abe-Arjun.Mallik\Downloads'

Software\Microsoft\Internet Explorer\AutoComplete
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)

Software\Microsoft\Internet Explorer\DOMStorage
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)
Subkeys:
  ams.hhs.gov            ---  Wed Apr 20 16:55:45 2016 UTC
  citrixonline.com       ---  Tue Apr 19 20:03:23 2016 UTC
  fda.gov                ---  Tue Apr 19 20:03:23 2016 UTC
  hhs.gov                ---  Wed Apr 20 16:55:45 2016 UTC
  hpsm.fda.gov           ---  Tue Apr 19 20:03:23 2016 UTC
  intranet.hhs.gov       ---  Tue Apr 19 20:03:23 2016 UTC
  login.citrixonline.com ---  Tue Apr 19 20:03:23 2016 UTC
  thehotfixshare.net     ---  Tue Apr 19 20:02:50 2016 UTC
  Total                  ---  Wed Apr 20 16:55:45 2016 UTC
  www.fda.gov            ---  Tue Apr 19 20:03:23 2016 UTC

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
  Internet Explorer version = 8.0.7601.19058

Software\Microsoft\Internet Explorer\Main
LastWrite Time Wed Apr 20 16:55:00 2016 (UTC)
  AllowWindowReuse                        = false [0]
  Anchor Underline                        = yes
  Cache_Update_Frequency                  = Once_Per_Session
  CompatibilityFlags                      = 0 [0x00000000]
  DefSpellLang                            = en-US
  Default_Page_URL                        = http://indside.fda.gov
                          Page 5

```
                              Admin OUTPUT.txt
   Disable Script Debugger            = yes
   DisableFirstRunCustomize           = 3
   DisableScriptDebuggerIE            = yes
   Display Inline Images              = yes
   Do404Search                        = 1 [0x01000000]
   DownloadWindowPlacement            = <skipped>
   Enable Browser Extensions          = yes
   FullScreen                         = no
   IE10RunOnceCompletionTime          = âò<`%Ñ
   IE10RunOncePerInstallCompleted     = 1
   IE8RunOnceLastShown                = true   [1]
   IE8RunOnceLastShown_TIMESTAMP      = Wed Dec 30 13:01:33 2015 UTC
   IE8RunOncePerInstallCompleted      = true   [1]
   ImageStoreRandomFolder             = fa7q1jq
   Local Page                         = C:\WINDOWS\system32\blank.htm
   NoSaveAsPOSTWarning                = 1
   NoUpdateCheck                      = true   [1]
   NotifyDownloadComplete             = yes
   OperationalData                    = |
   Play_Animations                    = yes
   Play_Background_Sounds             = yes
   Save_Session_History_On_Exit       = no
   Search Page                        =
http://go.microsoft.com/fwlink/?LinkId=54896
   Show_FullURL                       = no
   Show_StatusBar                     = yes
   Show_ToolBar                       = yes
   Show_URLToolBar                    = yes
   Show_URLinStatusBar                = yes
   Start Page                         = http://inside.fda.gov:9003/
   Use FormSuggest                    = no
   UseClearType                       = no
   Use_DlgBox_Colors                  = yes
   Window_Placement                   = <skipped>
   XMLHTTP                            = true   [1]

   Software\Microsoft\Internet Explorer\Main\WindowsSearch
   LastWrite Time Wed Apr 20 16:55:46 2016 (UTC)
      AutoCompleteGroups      = 5 [0x00000005]
      ConfiguredScopes        = 5 [0x00000005]
      LastCrawl               = Wed Apr 20 16:55:46 2016 UTC
      UpgradeTime             = Wed Apr 20 16:54:59 2016 UTC
      User Favorites Path     = file:///C:\Users\Abe-Arjun.Mallik\Favorites\
      Version                 = 6.1.7601.17610

Software\Microsoft\Internet Explorer\Privacy
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)
   CleanPassword             = true   [1]

Software\Microsoft\Internet Explorer\Recovery
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)

   Software\Microsoft\Internet Explorer\Recovery\Active
   LastWrite Time Wed Apr 20 16:56:42 2016 (UTC)
      {ABE232D3-B927-11E5-B55D-D4BED95C747D} = 0

   Software\Microsoft\Internet Explorer\Recovery\AdminActive
   LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

   Software\Microsoft\Internet Explorer\Recovery\PendingDelete
   LastWrite Time Wed Apr 20 16:56:42 2016 (UTC)

Software\Microsoft\Internet Explorer\Suggested Sites
                              Page 6
```

```
                              Admin OUTPUT.txt
LastWrite Time Wed Apr 20 16:55:00 2016 (UTC)
   DataStreamEnabledState         = 0
   Enabled                        = 0
   LogFileFolder                  =
C:\Users\Administrator\AppData\Local\Microsoft\windows\Temporary Internet Files\Low
   MigrationTime                  = Wed Apr 20 16:55:00 2016 UTC
   ObjectsCreated                 = false [0]
   ObjectsCreated_TIMESTAMP       = Wed Dec 30 13:01:45 2015 UTC

-----------------------------------------
internet_settings_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)
   AutoConfigProxy                = wininet.dll
   CertificateRevocation          = true   [1]
   DisableCachingOfSSLPages       = false [0]
   EmailName                      = User@
   EnableHttp1_1                  = true   [1]
   EnableNegotiate                = true   [1]
   IE5_UA_Backup_Flag             = 5.0
   MigrateProxy                   = true   [1]
   MimeExclusionListForCache      = multipart/mixed multipart/x-mixed-replace
multipart/x-byteranges
   PrivDiscUiShown                = true   [1]
   PrivacyAdvanced                = false [0]
   ProxyEnable                    = false [0]
   SecureProtocols                = 2688 [0x00000A80]
   UrlEncoding                    = false [0]
   UseSchannelDirectly            = 0x01000000
   User Agent                     = Mozilla/4.0 (compatible; MSIE 8.0; win32)
   WarnOnIntranet                 = true   [1]
   WarnOnPost                     = 0x01000000
   WarnonZoneCrossing             = false [0]
   ZonesSecurityUpgrade           = Wed Apr 20 12:57:37 2016 UTC


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
  LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
  LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
    AppContainerContentLimit  = 50
    AppContainerTotalContentLimit = 1000
    ContentLimit                   = 250
    Signature                      = Client UrlCache MMF Ver 5.2
    TotalContentLimit              = 0
    Version                        = 1

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
  LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)
    CacheLimit                     = 256000 KB
    CachePrefix                    =

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
  LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
    CacheLimit                     = 8192 KB
    CachePrefix                    = Cookie:

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
  LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
    CacheLimit                     = 8192 KB
```

Page 7

```
                                   Admin OUTPUT.txt
       CachePrefix                  = Visited:


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache
      LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DNTException
      LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)
        CacheLimit                  = 1 KB
        CacheOptions                = 0x300
        CachePath                   = %APPDATA%\Microsoft\Windows\DNTException
        CachePrefix                 = DNTException:
        CacheRepair                 = 0x0


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DOMStore
      LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
        CacheLimit                  = 1000 KB
        CacheOptions                = 0x8
        CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\DOMStore
        CachePrefix                 = DOMStore
        CacheRepair                 = 0x0


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieBrowserModeList
      LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)
        CacheLimit                  = 1 KB
        CacheOptions                = 0x300
        CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieBrowserModeList
        CachePrefix                 = EmieBrowserModeList:
        CacheRepair                 = 0x0


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieSiteList
      LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)
        CacheLimit                  = 1 KB
        CacheOptions                = 0x300
        CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieSiteList
        CachePrefix                 = EmieSiteList:
        CacheRepair                 = 0x0


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieUserList
      LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)
        CacheLimit                  = 1 KB
        CacheOptions                = 0x300
        CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieUserList
        CachePrefix                 = EmieUserList:
        CacheRepair                 = 0x0


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016042020160421
      LastWrite Time Wed Apr 20 12:59:06 2016 (UTC)
        CacheLimit                  = 8192 KB
        CacheOptions                = 0xB
        CachePath                   =
%USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042020
```

Page 8

Admin OUTPUT.txt
```
160421
     CachePrefix              = :2016042020160421:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\PrivacIE:
   LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
     CacheLimit               = 1024 KB
     CacheOptions             = 0x9
     CachePath                = %APPDATA%\Microsoft\Windows\PrivacIE
     CachePrefix              = PrivacIE:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\feedplat
   LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
     CacheLimit               = 8192 KB
     CacheOptions             = 0x0
     CachePath                = %USERPROFILE%\AppData\Local\Microsoft\Feeds Cache
     CachePrefix              = feedplat:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompat
   LastWrite Time Wed Apr 20 12:59:06 2016 (UTC)
     CacheLimit               = 1 KB
     CacheOptions             = 0x309
     CachePath                = %APPDATA%\Microsoft\Windows\IECompatCache
     CachePrefix              = iecompat:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompatua
   LastWrite Time Wed Apr 20 14:50:50 2016 (UTC)
     CacheLimit               = 1 KB
     CacheOptions             = 0x309
     CachePath                = %APPDATA%\Microsoft\Windows\iecompatuaCache
     CachePrefix              = iecompatua:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iedownload
   LastWrite Time Wed Apr 20 16:54:58 2016 (UTC)
     CacheLimit               = 8192 KB
     CacheOptions             = 0x9
     CachePath                = %APPDATA%\Microsoft\Windows\IEDownloadHistory
     CachePrefix              = iedownload:
     CacheRepair              = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\ietld
   LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
     CacheLimit               = 8192 KB
     CacheOptions             = 0x9
     CachePath                = %APPDATA%\Microsoft\Windows\IETldCache
     CachePrefix              = ietld:
     CacheRepair              = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
   LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Content
                                   Page 9
```

```
                              Admin OUTPUT.txt
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 256000 KB
       CachePrefix               =

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Cookies
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CachePrefix               = Cookie:

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\History
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CachePrefix               = Visited:


    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)

    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\EmieBrowserModeList
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CacheOptions              = 0x300
       CachePath                 = %USERPROFILE%\AppData\LocalLow\Microsoft\Internet
Explorer\EmieBrowserModeList
       CachePrefix               = EmieBrowserModeList:
       CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\EmieSiteList
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CacheOptions              = 0x300
       CachePath                 = %USERPROFILE%\AppData\LocalLow\Microsoft\Internet
Explorer\EmieSiteList
       CachePrefix               = EmieSiteList:
       CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\EmieUserList
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CacheOptions              = 0x300
       CachePath                 = %USERPROFILE%\AppData\LocalLow\Microsoft\Internet
Explorer\EmieUserList
       CachePrefix               = EmieUserList:
       CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\iecompat
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CacheOptions              = 0x309
       CachePath                 = %APPDATA%\Microsoft\Windows\IECompatCache\Low
       CachePrefix               = iecompat:
       CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\iecompatua
    LastWrite Time Wed Apr 20 16:55:02 2016 (UTC)
       CacheLimit                = 1 KB
       CacheOptions              = 0x309
```

Page 10

```
                                   Admin OUTPUT.txt
     CachePath                   = %APPDATA%\Microsoft\Windows\iecompatuaCache\Low
     CachePrefix                 = iecompatua:
     CacheRepair                 = 0x0


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\CACHE
 LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
     LastScavenge               = true  [1]
     LastScavenge_TIMESTAMP     = Tue Jan 12 13:44:10 2016 UTC
     Persistent                 = 1


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
 LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

 Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History
 LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
 ANALYST NOTE:
   No per-domain cookie decisions subkeys are present


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\Url History
 LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
     DaysToKeep                 = 40


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
 LastWrite Time Wed Apr 20 12:57:59 2016 (UTC)

   NETWORK SUBKEY: {51428976-C967-4527-8C08-8643694111E8}
   LastWrite Time Wed Apr 20 16:59:07 2016 (UTC)
     WpadDecision               = 0
     WpadDecisionReason         = 1
     WpadDecisionTime           = Wed Apr 20 16:59:07 2016 UTC
     WpadNetworkName            = fda.gov
     -- MAC SUBKEYS --
     00-08-e3-ff-fc-54          LastWritten Wed Apr 20 16:34:33 2016 UTC
     00-08-e3-ff-fc-54_1c-df-0f-2e-15-7f LastWritten Wed Apr 20 12:57:59 2016 UTC

   NETWORK SUBKEY: {4A85559C-33AC-4EE5-9C05-5EE34C61EE6F}
   LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)
     WpadDecision               = 0
     WpadDecisionReason         = 1
     WpadDecisionTime           = Tue Dec 29 19:16:57 2015 UTC
     WpadNetworkName            = fda.gov
     -- MAC SUBKEYS --
     64-f6-9d-e0-3c-bf          LastWritten Wed Apr 20 12:57:37 2016 UTC

   NETWORK SUBKEY: {3FDB7103-B989-4BDC-8196-1AEBEB99A8F8}
   LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
     WpadDecision               = 3
     WpadDecisionReason         = 1
     WpadDecisionTime           = Fri Dec  4 14:38:48 2015 UTC
     WpadNetworkName            = Abe-Arjun's iPhone (2)
     -- MAC SUBKEYS --
     7a-d7-5f-c0-b9-64          LastWritten Tue Apr 19 20:03:24 2016 UTC

   NETWORK SUBKEY:
{1F500AFF-5604-4DA3-943D-43D770ECEBD7}_{8254BA30-B8CE-48E7-932D-E58B23DDCB96}
   LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
     WpadDecision               = 0
     WpadDecisionReason         = 1
     WpadDecisionTime           = Tue Feb 16 12:13:28 2016 UTC
                              Page 11
```

```
                              Admin OUTPUT.txt
     WpadNetworkName          = FDA-WIFI
     -- MAC SUBKEYS --
     00-08-e3-ff-fc-54_1c-df-0f-2e-15-7f LastWritten Tue Apr 19 20:03:24 2016 UTC

    NETWORK SUBKEY:
{9767C410-13BF-4E09-96C5-5551E069A75B}_{CFBA167B-FB11-493B-8C21-8AC4FB31DC83}
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Fri Apr 15 18:17:29 2016 UTC
       WpadNetworkName         = fda.gov
       -- MAC SUBKEYS --
       00-11-22-33-44-55_e0-3f-49-9a-7b-40 LastWritten Tue Apr 19 20:03:24 2016 UTC

    NETWORK SUBKEY: {9767C410-13BF-4E09-96C5-5551E069A75B}
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Tue Apr 19 19:06:20 2016 UTC
       WpadNetworkName         = fda.gov
       -- MAC SUBKEYS --
       00-08-e3-ff-fc-54            LastWritten Tue Apr 19 20:03:24 2016 UTC
       00-08-e3-ff-fc-54_1c-df-0f-2e-15-7f LastWritten Tue Apr 19 20:03:24 2016 UTC
       00-08-e3-ff-fc-54_74-a2-e6-80-b6-bf LastWritten Tue Apr 19 20:03:24 2016 UTC
       00-11-22-33-44-55            LastWritten Tue Apr 19 20:03:24 2016 UTC
       1c-df-0f-2e-15-7f            LastWritten Tue Apr 19 20:03:24 2016 UTC

    NETWORK SUBKEY: {E21A3F01-4BE6-4FA8-BD11-0654ED5388B1}
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Fri Feb 12 20:15:12 2016 UTC
       WpadNetworkName        = Unidentified network
       -- MAC SUBKEYS --
       e0-3f-49-9a-7b-40            LastWritten Tue Apr 19 20:03:24 2016 UTC

    NETWORK SUBKEY: {CFBA167B-FB11-493B-8C21-8AC4FB31DC83}
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Fri Apr 15 12:16:49 2016 UTC
       WpadNetworkName         = Braddock
       -- MAC SUBKEYS --
       e0-3f-49-9a-7b-40            LastWritten Tue Apr 19 20:03:24 2016 UTC

    NETWORK SUBKEY: {B8602E23-66ED-4DBE-B6ED-89DEFA185B5A}
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Thu Aug  7 15:25:06 2014 UTC
       WpadNetworkName         = fda.gov
       -- MAC SUBKEYS --
       c4-7d-4f-a3-2a-7f            LastWritten Tue Apr 19 20:03:24 2016 UTC

    MACs SUBKEY: e0-3f-49-9a-7b-40
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
       WpadDecisionReason      = 1
       WpadDecisionTime        = Fri Apr 15 12:16:49 2016 UTC

    MACs SUBKEY: c4-7d-4f-a3-2a-7f
     LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
       WpadDecision           = 0
                              Page 12
```

```
                                Admin OUTPUT.txt
     WpadDecisionReason          = 1
     WpadDecisionTime            = Thu Aug  7 15:25:06 2014 UTC


   MACs SUBKEY: 7a-d7-5f-c0-b9-64
   LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
      WpadDecision               = 3
      WpadDecisionReason         = 1
      WpadDecisionTime           = Fri Dec  4 14:38:48 2015 UTC


   MACs SUBKEY: 1c-df-0f-2e-15-7f
   LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
      WpadDecision               = 0
      WpadDecisionReason         = 1
      WpadDecisionTime           = Tue Apr 19 19:06:20 2016 UTC


   MACs SUBKEY: 00-11-22-33-44-55
   LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
      WpadDecision               = 0
      WpadDecisionReason         = 1
      WpadDecisionTime           = Tue Apr 19 19:06:20 2016 UTC


   MACs SUBKEY: 64-f6-9d-e0-3c-bf
   LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)
      WpadDecision               = 0
      WpadDecisionReason         = 1
      WpadDecisionTime           = Tue Dec 29 19:16:57 2015 UTC


   MACs SUBKEY: 00-08-e3-ff-fc-54
   LastWrite Time Wed Apr 20 16:59:07 2016 (UTC)
      WpadDecision               = 0
      WpadDecisionReason         = 1
      WpadDecisionTime           = Wed Apr 20 16:59:07 2016 UTC
      WpadDetectedUrl            =


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
  LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
     (default)                   =
     AutoDetect                  = 1
     IntranetName                = 0
     ProxyByPass                 = 0
     UNCAsIntranet               = 0
     -- 'ZoneMap' subkeys -- not parsed:
        Domains                  Tue Apr 19 20:03:24 2016 UTC
        EscDomains               Tue Apr 19 20:02:50 2016 UTC
        ProtocolDefaults         Tue Apr 19 20:02:50 2016 UTC
        Ranges                   Tue Apr 19 20:02:50 2016 UTC

Subkeys not parsed in 'Software\Microsoft\Windows\CurrentVersion\Internet Settings'

     Activities          ---  Tue Apr 19 20:02:50 2016 UTC
     Connections         ---  Wed Apr 20 16:56:58 2016 UTC
     Http Filters        ---  Tue Apr 19 20:02:50 2016 UTC
     Lockdown_Zones      ---  Tue Apr 19 20:02:50 2016 UTC
     Passport            ---  Tue Apr 19 20:03:24 2016 UTC
     Protocols           ---  Tue Apr 19 20:02:50 2016 UTC
     TemplatePolicies    ---  Tue Apr 19 20:03:24 2016 UTC
     Zones               ---  Tue Apr 19 20:02:50 2016 UTC

------------------------------------------
javafx v.20110322
(NTUSER.DAT) Gets contents of user's JavaFX key
```

Page 13

Admin OUTPUT.txt

javafx v.20110322
Software\JavaSoft\Java Update\Policy\JavaFX
LastWrite time: Wed Apr 20 13:02:44 2016

UpdateSchedule            6
UpdateScheduleMinutes     26
Frequency                 4
------------------------------------
listsoft v.20080324
(NTUSER.DAT) Lists contents of user's Software key

listsoft v.20080324
List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

Wed Apr 20 16:28:56 2016Z       Cisco Systems, Inc.
Wed Apr 20 15:42:01 2016Z       Mozilla
Wed Apr 20 15:41:29 2016Z       Microsoft
Wed Apr 20 15:41:27 2016Z       Policies
Wed Apr 20 15:01:08 2016Z       Clients
Wed Apr 20 13:09:33 2016Z       Adobe
Wed Apr 20 13:02:44 2016Z       JavaSoft
Wed Apr 20 12:59:16 2016Z       Google
Wed Apr 20 12:59:09 2016Z       KONICA MINOLTA
Wed Apr 20 12:59:00 2016Z       McAfee
Wed Apr 20 12:57:49 2016Z       Alps
Wed Apr 20 12:57:43 2016Z       NVIDIA Corporation
Wed Apr 20 12:57:42 2016Z       Realtek
Wed Apr 20 12:57:32 2016Z       FDA
Wed Apr 20 12:57:32 2016Z       KiXtart
Wed Apr 20 12:57:30 2016Z       Intel
Tue Apr 19 20:03:24 2016Z       ODBC
Tue Apr 19 20:02:50 2016Z       AppDataLow
Tue Apr 19 20:02:50 2016Z       EMC
Tue Apr 19 20:02:50 2016Z       IM Providers
Tue Apr 19 20:02:50 2016Z       Wow6432Node
------------------------------------
liveContactsGUID v.20110221
(NTUSER.DAT) Gets user Windows Live Messenger GUIDs

Software\Microsoft\Windows Live Contacts\Database not found.
------------------------------------
load v.20100811
(NTUSER.DAT) Gets load and run values from user hive

load
Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Apr 20 12:57:39 2016 (UTC)

load value not found.
run value not found.
------------------------------------
logonusername v.20080324
(NTUSER.DAT) Get user's Logon User Name value

Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Wed Apr 20 15:41:38 2016 (UTC)]
------------------------------------
mmc v.20080324
(NTUSER.DAT) Get contents of user's MMC\Recent File List key

MMC - Recent File List

Page 14

```
                       Admin OUTPUT.txt
Software\Microsoft\Microsoft Management Console\Recent File List
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
   File1 -> C:\windows\System32\services.msc
-----------------------------------------
mndmru v.20080324
(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.
-----------------------------------------
mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Wed Apr 20 13:02:41 2016 (UTC)

Remote Drives:
Wed Apr 20 13:02:41 2016 (UTC)
   ##fda.gov#wodc#OC#Users02#Abe-Arjun.Mallik
   ##OCS03#Apps
Tue Apr 19 20:02:50 2016 (UTC)
   ##FDSWPCM04264#DeploymentShare$

Volumes:
Tue Apr 19 20:02:50 2016 (UTC)
   {f77e7eee-ae5b-11e5-9806-806e6f6e6963}
   {f77e7ef1-ae5b-11e5-9806-806e6f6e6963}

Drives:
Tue Apr 19 20:02:50 2016 (UTC) - CPC

Unique MAC Addresses:
80:6E:6F:6E:69:63

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices
entries that begin with "\??\Volume".
-----------------------------------------
mpmru v.20080324
(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.
-----------------------------------------
mspaper v.20080324
(NTUSER.DAT) Gets images listed in user's MSPaper key

SOFTWARE\Microsoft\MSPaper* not found.
-----------------------------------------
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
-----------------------------------------
nero v.20100218
(NTUSER.DAT) Gets contents of Ahead\Nero Recent File List subkeys

Software\Ahead not found.
-----------------------------------------
netassist v.20110427
(NTUSER.DAT) Check for Firefox Extensions.

Software\Mozilla\Firefox\Extensions not found.
                       Page 15
```

Admin OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Uninstall\NetAssistant not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0 not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0\SourceList
not found.

```
------------------------------------
```
odysseus v.20110202
(NTUSER.DAT) Extract registry keys for Odysseus by bindshell.net.

Software\bindshell.net\Odysseus not found.

```
------------------------------------
```
officedocs v.20080324
(NTUSER.DAT) Gets contents of user's Office doc MRU keys

officedocs v.20080324
MSOffice version not found.
```
------------------------------------
```
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version 2010 located.
Software\Microsoft\Office\14.0\Word\File MRU
LastWrite Time Wed Apr 20 15:43:30 2016 (UTC)
    Item 1 -> C:\Users\Abe-Arjun.Mallik\Documents\April 2016 LMM Final 04-05-2016.docx
 Wed Apr 20 14:50:43 2016
    Item 2 -> E:\Current Event Summary    Nikita Mallik#16.docx  Thu Apr 14 12:37:06
2016
    Item 3 -> C:\Users\Abe-Arjun.Mallik\Documents\Report of Survey Clearance Form.doc
Wed Apr 13 19:28:12 2016
    Item 4 ->
http://inside.fda.gov:9003/downloads/AboutFDA/FDAStaffInformation/OrgCharts/UCM26286
1.doc  Tue Apr 12 19:16:38 2016
    Item 5 ->
http://inside.fda.gov:9003/downloads/AboutFDA/FDAStaffInformation/OrgCharts/UCM26297
1.docx  Tue Apr 12 19:16:11 2016
    Item 6 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Center contacts.doc  Mon Apr 11
15:23:44 2016
    Item 7 -> C:\Users\Abe-Arjun.Mallik\Documents\Misc\Resume Mallik.doc  Wed Apr  6
15:39:02 2016
    Item 8 -> C:\Users\Abe-Arjun.Mallik\Documents\payroll.doc  Wed Apr  6 13:38:49
2016
    Item 9 -> C:\Users\Abe-Arjun.Mallik\Documents\2015 September LMM Final
09-29-2015.docx  Wed Apr  6 12:12:18 2016
    Item 10 -> C:\Users\Abe-Arjun.Mallik\Documents\2015 LMM 12-18-2015 clean docx.docx
 Tue Apr  5 18:13:17 2016
    Item 11 -> C:\Users\Abe-Arjun.Mallik\Documents\April 2016 LMM Final.docx  Tue Apr
5 16:22:35 2016
    Item 12 -> C:\Users\Abe-Arjun.Mallik\Documents\AAC Request FDA HHS.docx  Tue Apr
5 15:58:51 2016
    Item 13 -> C:\Users\Abe-Arjun.Mallik\Documents\Agenda - NCTR meeting 04-5-16.docx
Tue Apr  5 14:53:00 2016
    Item 14 -> C:\Users\Abe-Arjun.Mallik\Documents\DONOT_DISTURB.doc  Tue Apr  5
12:48:40 2016
    Item 15 -> C:\Users\Abe-Arjun.Mallik\Documents\Agenda - Deanna meeting
03-15-16.docx  Mon Apr  4 19:00:40 2016
    Item 16 -> C:\Users\Abe-Arjun.Mallik\Documents\Say what.doc  Mon Apr  4 16:16:30
2016
    Item 17 ->
http://inside.fda.gov:9003/downloads/EmployeeResources/Training/ITTraining-GeneralIn
formation/UCM447072.docx  Mon Apr  4 11:34:28 2016
    Item 18 -> C:\Users\Abe-Arjun.Mallik\Documents\Misc\Agreement for Lawn
Maintenance.doc  Fri Apr  1 15:03:35 2016

Page 16

Admin OUTPUT.txt

Item 19 -> C:\Users\Abe-Arjun.Mallik\Documents\2016 April LMM Final.docx   Fri Apr 1 14:19:24 2016
Item 20 -> C:\Users\Abe-Arjun.Mallik\Documents\Abandonment and Destruction Certification.doc  Mon Mar 28 19:25:42 2016
Item 21 -> C:\Users\Abe-Arjun.Mallik\Documents\NCTR Guide to Reutilization and Disposition 30-25-16.docx  Mon Mar 28 19:06:08 2016
Item 22 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Guide to Reutilization and Disposition.docx  Mon Mar 28 19:04:04 2016
Item 23 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Guide to Reutilization and Disposition 30-24-16.docx  Mon Mar 28 19:03:43 2016
Item 24 -> C:\Users\Abe-Arjun.Mallik\Documents\JOB SUMMARY.doc  Mon Mar 28 14:12:17 2016
Item 25 -> C:\Users\Abe-Arjun.Mallik\Documents\Personal Property Specialist.doc  Mon Mar 28 14:09:48 2016
Item 26 -> http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Documents/PPMO%20WebEx%20Credentials/PPMO%20WebEx%20Credentials.doc  Fri Mar 25 18:28:39 2016
Item 27 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Guide to Reutilization and Disposition 30-25-16.docx  Fri Mar 25 14:15:05 2016
Item 28 -> C:\Users\Abe-Arjun.Mallik\Documents\Misc\Laptop Security.doc  Fri Mar 25 14:13:29 2016
Item 29 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Guide to Reutilization and Disposition 30-23-16.docx  Wed Mar 23 13:06:30 2016
Item 30 -> C:\Users\Abe-Arjun.Mallik\Documents\Misc\Laptop Hard Drive.doc  Wed Mar 23 12:08:05 2016
Item 31 -> C:\Users\Abe-Arjun.Mallik\Documents\FederalGuideReutilizationandDispositionofExcess.docx  Tue Mar 22 11:36:13 2016
Item 32 -> C:\Users\Abe-Arjun.Mallik\Documents\Summary of GSAXcess.doc  Mon Mar 21 19:20:54 2016
Item 33 -> C:\Users\Abe-Arjun.Mallik\Documents\JJS pay2015.doc  Mon Mar 21 14:27:06 2016
Item 34 -> E:\EEO\EEO 2014\Petitioners response to Agency Discovery.docx  Mon Mar 21 13:10:44 2016
Item 35 -> E:\EEO\Mallik Formal Complaint 2014.doc  Mon Mar 21 12:47:04 2016
Item 36 -> E:\EEO\EEO 2014\Affidavit Mallik protected.docx  Mon Mar 21 11:20:54 2016
Item 37 -> http://inside.fda.gov:9003/downloads/administrative/forms/fda/ucm014650.doc  Fri Mar 18 22:36:02 2016
Item 38 -> http://inside.fda.gov:9003/downloads/cder/officeofmanagement/divisionofmanagementservices/ucm453057.doc  Fri Mar 18 12:12:16 2016
Item 39 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT\Combined - Internal Strengths.doc  Fri Mar 18 11:35:42 2016
Item 40 -> http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Documents/SWOT/Combined%20-%20External%20Opportunities.doc  Fri Mar 18 11:35:14 2016
Item 41 -> http://inside.fda.gov:9003/downloads/administrative/budgetfinance/cvmbudgetfinance/ucm055568.doc  Fri Mar 18 00:02:04 2016
Item 42 -> C:\Users\Abe-Arjun.Mallik\Documents\Designation Letter - Survey Officer 03152016.doc  Wed Mar 16 13:57:27 2016
Item 43 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess FDA Blank Form.doc  Tue Mar 15 17:04:10 2016
Item 44 -> C:\Users\Abe-Arjun.Mallik\Documents\Doc1.doc  Tue Mar 15 17:00:43 2016
Item 45 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess Program Steps.doc  Tue Mar 15 16:57:54 2016
Item 46 -> C:\Users\Abe-Arjun.Mallik\Documents\Metlife EOB.doc  Tue Mar 15 12:05:46 2016
Item 47 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT\Combined - External Threats.doc  Mon Mar 14 19:24:31 2016
Item 48 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT\Combined - External

Page 17

Admin_OUTPUT.txt
Opportunities.doc  Mon Mar 14 19:24:09 2016
    Item 49 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT\Combined - Internal
Weakness.doc  Mon Mar 14 19:23:58 2016
    Item 50 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT\SWOT- Gwen CDER.doc  Mon Mar
14 19:23:22 2016

Software\Microsoft\Office\14.0\Excel\File MRU
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)
    Item 1 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Action%20Tracker/PPMO%20Action%2
0Tracker%20Log.xls  Mon Apr 18 18:28:04 2016
    Item 2 -> C:\Users\Abe-Arjun.Mallik\Documents\Mallik Timesheet.xls  Wed Apr  6
13:39:40 2016
    Item 3 -> C:\Users\Abe-Arjun.Mallik\Documents\2015 FDA Final Inventory.xlsx  Mon
Mar 14 14:08:59 2016
    Item 4 -> C:\Users\Abe-Arjun.Mallik\Documents\Inventory Analysis.xlsx  Mon Mar 14
14:08:27 2016
    Item 5 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2015.xlsx  Mon Mar
14 14:07:33 2016
    Item 6 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Complete Asset Listing.xlsx  Mon
Mar 14 13:58:01 2016
    Item 7 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Complete Asset Listing - no
blanks.xlsx  Mon Mar 14 13:57:46 2016
    Item 8 -> C:\Users\Abe-Arjun.Mallik\Desktop\2016 Timesheet.xls  Wed Mar  9
12:55:23 2016
    Item 9 -> C:\Users\Abe-Arjun.Mallik\Documents\NCTR and CTP Summary OC31.xlsx  Fri
Mar  4 13:33:59 2016
    Item 10 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA AAC Codes - 01-28-2016.xlsx
Tue Mar  1 14:31:34 2016
    Item 11 -> C:\Users\Abe-Arjun.Mallik\Documents\TRAVEL PLAN MASTER FY2016.xls  Tue
Mar  1 12:17:17 2016
    Item 12 -> C:\Users\Abe-Arjun.Mallik\Documents\Mughals.xlsx  Thu Feb 25 13:05:40
2016
    Item 13 -> C:\Users\Abe-Arjun.Mallik\Downloads\ext_user_administration.xls  Wed
Feb 24 17:26:09 2016
    Item 14 -> C:\Users\Abe-Arjun.Mallik\Documents\rwservlet.xls  Wed Feb 24 14:52:11
2016
    Item 15 -> C:\Users\Abe-Arjun.Mallik\Documents\2016 Timesheet.xls  Wed Feb 24
12:21:31 2016
    Item 16 -> C:\Users\Abe-Arjun.Mallik\Documents\timesheet PPE 23.xlsx  Wed Feb 24
12:21:10 2016
    Item 17 -> C:\Users\Abe-Arjun.Mallik\Documents\Report 14 02-10-2016.xlsx  Mon Feb
22 15:47:40 2016
    Item 18 -> C:\Users\Abe-Arjun.Mallik\Documents\ext_user_administration.xls  Wed
Feb 17 13:35:08 2016
    Item 19 ->
https://assetweb.psc.gov/reports/rwservlet?cmdkey=snflwr_04050000_report_psc&server=
repl1g_snflwr_04050000_psc&destype=cache&p_user_id=50154596478&report=PMIS_Annual_As
sets_Summary.rdf&p_org_ID=50003034344&p_year=2015&mode=default&DESFORMAT=spreadsheet
Tue Feb 16 14:12:07 2016
    Item 20 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/ATF/02-10-16/2016%20Inventory%20Schedul
e.xls  Mon Feb  8 18:37:24 2016
    Item 21 -> C:\Users\Abe-Arjun.Mallik\Documents\PMIS users.xlsx  Wed Feb  3
15:40:18 2016
    Item 22 -> C:\Users\Abe-Arjun.Mallik\Documents\IGCE Terathink.xlsx  Fri Jan 22
19:43:59 2016
    Item 23 -> C:\Users\Abe-Arjun.Mallik\Documents\IGCE sample sheet.xls  Fri Jan 22
18:17:12 2016
    Item 24 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA Weapons.xls  Tue Jan 12
19:47:55 2016
    Item 25 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2015 a .xlsx  Tue
Jan 12 14:10:20 2016

Page 18

Admin OUTPUT.txt

 Item 26 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2011 a .xlsx   Tue Jan 12 13:54:24 2016
 Item 27 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2012 a .xlsx   Tue Jan 12 13:52:30 2016
 Item 28 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2013 a .xlsx   Tue Jan 12 13:51:10 2016
 Item 29 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2014 a .xlsx   Tue Jan 12 13:49:49 2016
 Item 30 -> C:\Users\Abe-Arjun.Mallik\Documents\All Assets report 2014.xlsx   Tue Jan 12 13:43:06 2016
 Item 31 -> C:\Users\Abe-Arjun.Mallik\Desktop\file2.txt   Tue Jan 12 13:31:06 2016
 Item 32 -> C:\Users\Abe-Arjun.Mallik\Desktop\file1.txt   Tue Jan 12 13:19:15 2016
 Item 33 -> C:\Users\Abe-Arjun.Mallik\Desktop\PMIS all Assets.txt   Mon Jan 11 16:01:21 2016
 Item 34 -> C:\Users\Abe-Arjun.Mallik\Documents\Copy of timesheet (2).xlsx   Thu Jan 7 17:02:03 2016
 Item 35 -> C:\Users\Abe-Arjun.Mallik\Documents\Rivers.xls   Wed Jan  6 14:38:59 2016
 Item 36 -> C:\Users\Abe-Arjun.Mallik\Documents\Capitals.xls   Wed Jan  6 14:31:01 2016
 Item 37 -> http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Documents/PPM%20Assett%20Portfolio.xls   Wed Jan  6 14:09:03 2016
 Item 38 -> C:\Users\Abe-Arjun.Mallik\Documents\PPM Assett Portfolio.xls   Wed Jan 6 13:46:03 2016
 Item 39 -> C:\Users\Abe-Arjun.Mallik\Desktop\timesheet.xlsx   Wed Jan  6 12:11:58 2016
 Item 40 -> C:\Users\Abe-Arjun.Mallik\Documents\Estate.xls   Mon Jan  4 13:52:30 2016
 Item 41 -> C:\Users\Abe-Arjun.Mallik\Documents\APO Contact Info.xls   Wed Dec 16 14:24:03 2015
 Item 42 -> C:\Users\Abe-Arjun.Mallik\Documents\Mallik FDATravelerProfilesTEMPLATE.xlsx   Wed Dec 16 14:03:56 2015
 Item 43 -> C:\Users\Abe-Arjun.Mallik\Documents\ACC FDA Addresses updated 12-01-2015.xls   Wed Dec 16 13:16:00 2015
 Item 44 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA NWJ Updates.xls   Thu Dec 10 16:32:55 2015
 Item 45 -> C:\Users\Abe-Arjun.Mallik\Documents\fda GSAXcess FDA user list.xml.xls   Tue Dec  8 19:22:23 2015
 Item 46 -> http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/Shared%20Documents/Latest%20APO%20Listing_August%2019,%202015.xlsx   Thu Dec  3 15:09:30 2015
 Item 47 -> C:\Users\Abe-Arjun.Mallik\Documents\FDA ACC listing.xlsx   Wed Dec  2 16:47:53 2015
 Item 48 -> C:\Users\Abe-Arjun.Mallik\Documents\ACC FDA Addresses.xls   Tue Dec  1 18:26:56 2015
 Item 49 -> http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Action%20Tracker/PPMO%20Action%20Tracker%20Log%20(Autosaved).xls   Wed Nov 18 14:48:13 2015
 Item 50 -> C:\Users\Abe-Arjun.Mallik\Documents\PPMO travel cost for 2016.xls   Tue Nov 17 18:43:34 2015

Software\Microsoft\Office\14.0\Access\File MRU
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)
Software\Microsoft\Office\14.0\Access\File MRU has no values.

Software\Microsoft\Office\14.0\PowerPoint\File MRU
LastWrite Time Tue Apr 19 20:03:21 2016 (UTC)
 Item 1 -> C:\Users\Abe-Arjun.Mallik\Documents\LAPTOP REFRESH PROCESS-2.ppt   Thu Apr 14 15:24:37 2016
 Item 2 -> C:\Users\Abe-Arjun.Mallik\Documents\Property Custodial Officer 2016.ppt Wed Apr 13 16:35:04 2016
 Item 3 -> C:\Users\Abe-Arjun.Mallik\Documents\Re-Utilization & Disposal History -

Page 19

Admin OUTPUT.txt

Process.ppt  Wed Apr 13 11:28:55 2016
    Item 4 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess Property brief.ppt  Tue Apr
12 11:39:21 2016
    Item 5 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess Property.ppt  Tue Apr 12
11:38:44 2016
    Item 6 -> C:\Users\Abe-Arjun.Mallik\Documents\Abandonment and Destruction.ppt  Tue
Apr 12 11:38:30 2016
    Item 7 -> C:\Users\Abe-Arjun.Mallik\Documents\Personal Property Disposal
Overview.ppt  Tue Apr 12 11:38:19 2016
    Item 8 ->
C:\Users\Abe-Arjun.Mallik\Documents\Presentations\June_24_1345_Buchar_PM_101_.pptx
Mon Apr 11 19:13:33 2016
    Item 9 -> C:\Users\Abe-Arjun.Mallik\Documents\Presentations\BM1EOC.ppt  Mon Apr 11
19:13:08 2016
    Item 10 ->
C:\Users\Abe-Arjun.Mallik\Documents\Presentations\Physical_Inventory.ppt  Mon Apr 11
18:45:15 2016
    Item 11 ->
C:\Users\Abe-Arjun.Mallik\Documents\Presentations\CAPETEvidenceClass.ppt  Mon Apr 11
18:44:20 2016
    Item 12 ->
C:\Users\Abe-Arjun.Mallik\Documents\Presentations\NES12-123GovtPropertyInMoti.pptx
Mon Apr 11 18:43:22 2016
    Item 13 -> C:\Users\Abe-Arjun.Mallik\Documents\Presentations\CSDP CDR CRSE
Slides.ppt  Mon Apr 11 18:42:14 2016
    Item 14 -> C:\Users\Abe-Arjun.Mallik\Documents\Presentations\J_GSAAuctions.ppt
Mon Apr 11 18:40:57 2016
    Item 15 -> C:\Users\Abe-Arjun.Mallik\Documents\PPD_Overview.pptx  Tue Apr  5
11:17:30 2016
    Item 16 -> C:\Users\Abe-Arjun.Mallik\Documents\Personal Property Mgmt _NEO
9-01-15.pptx  Wed Mar 30 16:42:05 2016
    Item 17 -> C:\Users\Abe-Arjun.Mallik\Documents\xcessSearchProp.ppt  Wed Mar 30
16:40:54 2016
    Item 18 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess Property ORA.ppt  Wed Mar
30 16:38:10 2016
    Item 19 -> C:\Users\Abe-Arjun.Mallik\Documents\LAPTOP REFRESH PROCESS.ppt  Wed Mar
30 15:41:49 2016
    Item 20 -> C:\Users\Abe-Arjun.Mallik\Documents\LAPTOP REFRESH PROCESS with
animation.ppt  Wed Mar 30 15:08:29 2016
    Item 21 -> C:\Users\Abe-Arjun.Mallik\Documents\SWOT PPMO-Abe.ppt  Wed Feb 17
14:44:17 2016
    Item 22 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/ROS1/Report%20of%20Survey%20Training%20
-%20Abe%20Final.ppt  Tue Feb 16 18:10:50 2016
    Item 23 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/ROS1/Report%20of%20Survey%20Training%20
-%20Abe.ppt  Tue Feb 16 17:37:49 2016
    Item 24 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/ROS1/Report%20of%20Survey%20Training.pp
t  Tue Feb 16 13:06:24 2016
    Item 25 -> C:\Users\Abe-Arjun.Mallik\Documents\GSAXcess Property ORA Nov 2015.ppt
Mon Jan  4 17:31:31 2016
    Item 26 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/Accomplishments/2015%20PCO%20All-Hands%
20Meeting.ppt  Wed Dec  2 13:37:05 2015
    Item 27 ->
http://inside.fda.gov:9003/downloads/administrative/budgetfinance/ofmbudgetofficersp
ortal/ucm464661.pptx  Mon Nov 30 16:56:38 2015
    Item 28 -> C:\Users\Abe-Arjun.Mallik\Documents\Property Validation ORA.ppt  Tue
Nov 17 15:23:44 2015
    Item 29 -> C:\Users\Abe-Arjun.Mallik\Documents\DFTPS-PG FDA Presentation 1-31 wo
tech.ppt  Mon Nov  9 15:05:40 2015
    Item 30 -> C:\Users\Abe-Arjun.Mallik\AppData\Local\Temp\3\wz13e3\OFEMS

```
                        Admin OUTPUT.txt
meeting\Property Management Presentation_OFEMS.pptx   Mon Nov  2 15:16:44 2015
   Item 31 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/New%20Employee%20Orientation%20NEO/Pers
onal%20Property%20Mgmt%20_NEO%209-01-15.pptx  Mon Nov  2 13:06:10 2015
   Item 32 -> Y:\Documents\DFTPS-PG FDA Presentation 1-31 wo tech.ppt  Thu Oct  8
19:24:07 2015
---------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

MSOffice version not found.
---------------------------------------
OSVersion
Software\Microsoft
LastWrite Time Wed Apr 20 15:41:29 2016 (UTC)

OSVersion value not found.
---------------------------------------
outlook v.20100218
(NTUSER.DAT) Gets user's Outlook settings


Outlook Profile
---------------------------------------
policies_u v.20091021
(NTUSER.DAT) Get values from the user's Policies key


Explorer subkey values:
   HideSCAHealth             1
   ForceRunOnStartMenu   1
   NoDriveTypeAutoRun     255
   ForceClassicControlPanel 1
   ForceStartMenuLogOff 1
   Intellimenus              1
   NoAutoTrayNotify          1
   NoDesktopCleanupWizard 1
   NoWelcomeScreen           1
   NoInplaceSharing          1

System\EnableProfileQuota value not found.
---------------------------------------
printermru v.20091125
(NTUSER.DAT) Gets user's Printer Wizard MRU listing

Printers\Settings\Wizard\ConnectMRU
LastWrite Time Tue Apr 19 20:03:23 2016 (UTC)

Printers listed in MRUList order.
   a -> \\fdswv03876
---------------------------------------
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Wed Apr 20 15:41:30 2016

   Microsoft XPS Document Writer (winspool,Ne01:,15,45)
   Fax (winspool,Ne01:,15,45)
   Send To OneNote 2010 (winspool,nul:,15,45)
   \\fdswv03876\FDPKO161 (winspool,Ne03:,15,45)
   \\fdswv03876\FDPKO168 (winspool,Ne04:,15,45)
   Adobe PDF (winspool,Ne02:,15,45)
                              Page 21
```

```
                              Admin OUTPUT.txt
   hp deskjet 5550 series (HPA) (winspool,Ne01:,15,45)
   WebEx Document Loader (winspool,Ne00:,15,45)

Default Printer (via CurrentVersion\Windows): \\fdswv03876\FDPKO168,winspool,Ne04:
----------------------------------------------
privoxy v.20110204
(NTUSER.DAT) Extracts the install path for Privoxy.

Software\Privoxy not found.


----------------------------------------------
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Wed Apr 20 12:57:37 2016 (UTC)
   AutoConfigProxy                 wininet.dll
   CertificateRevocation           1
   DisableCachingOfSSLPages        0
   EmailName                       User@
   EnableHttp1_1                   1
   EnableNegotiate                 1
   IE5_UA_Backup_Flag              5.0
   MigrateProxy                    1
   MimeExclusionListForCache       multipart/mixed multipart/x-mixed-replace
multipart/x-byteranges
   PrivDiscUiShown                 1
   PrivacyAdvanced                 0
   ProxyEnable                     0
   SecureProtocols                 2688
   UrlEncoding                     0
   UseSchannelDirectly             1
   User Agent                      Mozilla/4.0 (compatible; MSIE 8.0; Win32)
   WarnOnIntranet                  1
   WarnOnPost                      1
   WarnonZoneCrossing              0
   ZonesSecurityUpgrade            923740076
----------------------------------------------
publishingwizard v.20110202
(NTUSER.DAT) Extract AddNetPlace\LocationMRU for Microsoft Publishing Wizard

Software\Microsoft\Windows\CurrentVersion\Explorer\PublishingWizard\AddNetworkPlace\
AddNetPlace\LocationMRU not found.


----------------------------------------------
putty v.20110204
(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.


----------------------------------------------
rdphint v.20090715
(NTUSER) Gets hosts logged onto via RDP and the Domain\Username

Software\Microsoft\Terminal Server Client\Servers not found.
----------------------------------------------
realplayer6 v.20080324
(NTUSER.DAT) Gets user's RealPlayer v6 MostRecentClips(Default) values

Software\RealNetworks\RealPlayer\6.0\Preferences not found.
----------------------------------------------
realvnc v.20091125
```

Admin OUTPUT.txt
(NTUSER.DAT) Gets user's RealVNC MRU listing

Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Apr 20 14:53:50 2016 (UTC)
  0 = April 2016 LMM Final 04-05-2016.docx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time Wed Apr 20 14:53:50 2016 (UTC)
MRUListEx = 0
  0 = April 2016 LMM Final 04-05-2016.docx


------------------------------------------
rootkit_revealer v.20110204
(NTUSER.DAT) Extracts the EULA value for Sysinternals Rootkit Revealer.

Software\Sysinternals\RootkitRevealer not found.

------------------------------------------
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Wed Apr 20 13:23:56 2016 (UTC)
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU has no values.
------------------------------------------
Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
------------------------------------------
shellfolders v.20090115
(NTUSER.DAT) Retrieve user Shell Folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
LastWrite Time Wed Apr 20 12:57:39 2016 (UTC)
!Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath
function instead
AppData            C:\Users\Abe-Arjun.Mallik\AppData\Roaming
Local AppData      C:\Users\Abe-Arjun.Mallik\AppData\Local
My Video           C:\Users\Abe-Arjun.Mallik\Videos
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Libraries
My Pictures        C:\Users\Abe-Arjun.Mallik\Pictures
Desktop            C:\Users\Abe-Arjun.Mallik\Desktop
History
C:\Users\Abe-Arjun.Mallik\AppData\Local\Microsoft\Windows\History
NetHood
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Network Shortcuts
{56784854-C6CB-462B-8169-88E350ACB882} C:\Users\Abe-Arjun.Mallik\Contacts
Cookies
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Cookies
Favorites          C:\Users\Abe-Arjun.Mallik\Favorites
SendTo
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Start Menu
My Music           C:\Users\Abe-Arjun.Mallik\Music
Page 23

```
                              Admin OUTPUT.txt
Programs
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Recent
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Recent
CD Burning
C:\Users\Abe-Arjun.Mallik\AppData\Local\Microsoft\Windows\Burn\Burn
PrintHood
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\Abe-Arjun.Mallik\Searches
{374DE290-123F-4565-9164-39C4925E467B} C:\Users\Abe-Arjun.Mallik\Downloads
{A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\Abe-Arjun.Mallik\AppData\LocalLow
Startup
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Administrative Tools
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
Personal                C:\Users\Abe-Arjun.Mallik\Documents
{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\Abe-Arjun.Mallik\Links
Cache                   C:\Users\Abe-Arjun.Mallik\Documents\Browsing\Temporary Internet
Files
Templates
C:\Users\Abe-Arjun.Mallik\AppData\Roaming\Microsoft\Windows\Templates
{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\Abe-Arjun.Mallik\Saved Games
Fonts                   C:\WINDOWS\Fonts


-----------------------------------------
Software\Skype not found.
-----------------------------------------
snapshot_viewer v.20110210
(NTUSER.DAT) Extracts Recent File List for Microsoft Snapshot Viewer.

Software\Microsoft\Snapshot Viewer\Recent File List not found.


-----------------------------------------
ssh_host_keys v.20120809
(NTUSER.DAT) Extracts Putty/WinSCP SSH Host Keys

"Software\SimonTatham\Putty\SshHostKeys" does not exist

"Software\Martin Prikryl\WinSCP 2\SshHostKeys" does not exist
-----------------------------------------
startmenuinternetapps_cu v.20101219
(NTUSER.DAT) Start Menu Internet Applications info current user

Start Menu Internet Applications

StartMenuInternet [Wed Apr 20 15:01:08 2016 (UTC)]
NOTE: default Internet Browser client key
(default) -> FIREFOX.EXE


-----------------------------------------
startpage v.20100330
(NTUSER.DAT) Gets contents of user's StartPage key

Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage
LastWrite Time Wed Apr 20 12:57:41 2016 (UTC)

StartMenu_Start_Time   = Wed Apr 20 12:57:41 2016 Z
StartMenu_Balloon_Time = Tue Apr 19 19:13:29 2016 Z
-----------------------------------------
streammru v.20090205
(NTUSER.DAT) streammru
```

Page 24

Admin OUTPUT.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
------------------------------------------
streams v.20081124
(NTUSER.DAT) Parse Streams and StreamsMRU entries

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
------------------------------------------
Software\SysInternals not found.
------------------------------------------
trustrecords v.20120716
word
LastPurgeTime = Fri Oct  9 20:36:59 1970
Thu Oct 29 14:19:09 2015 ->
%USERPROFILE%/Documents/2015%20LMM%20Revised%20040515.docx
Fri Jan 29 22:54:31 2016 ->
%USERPROFILE%/Documents/Report%20of%20Survey%20within%20FDA.docx
Mon Oct 26 12:31:36 2015 ->
file:///E:/6726/Tenants/6726%20Jefferson%20Blvd%20Lease%20Agreement-%20Guillory.doc
Wed Nov  4 14:38:02 2015 ->
file:///E:/6726/Tenants/6726%20Jefferson%20Blvd%20Lease%20Agreement-%20Thurman.doc

PowerPoint
LastPurgeTime = Fri Oct  9 17:06:39 1970

Excel
LastPurgeTime = Fri Oct  9 19:54:26 1970

Access

------------------------------------------
Launching tsclient v.20120827
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
------------------------------------------
typedpaths v.20100330
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
------------------------------------------
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
  url1 -> http://www.yahoo.com/
  url2 -> http://www.google.com/
  url3 -> http://www.gsa.gov/portal/category/22227
  url4 -> http://tiny.cc/yey49x
  url5 -> https://faitas.army.mil/Faitas/
  url6 -> https://www.surveymonkey.com/r/TALEXApplication
  url7 ->
https://interact.gsa.gov/user/reset/225010/1458669492/ymSguhZM2qC_5PSHrB6Um_ggg7zS4B
IhkQ8w7u3X0Mw
  url8 -> http://intranet.fda.gov/omp/smg/guides-manuals.htm
  url9 ->

Page 25

Admin OUTPUT.txt
http://inside.fda.gov:9003/PolicyProcedures/StaffManualGuide/IssuingStaffManualGuide
s/ucm019808.htm
    url10 -> http://gsaxcess.gov/fedsweb/pubw2100/
    url11 -> https://calendar.google.com/calendar
    url12 -> http://www.gsa.gov/fedfleet
    url13 -> https://efds.hhs.gov/
    url14 -> http://gsa.gov/
    url15 -> http://www.govsales.gov/
    url16 -> http://fda.webex.com/
    url17 ->
http://rqst-it.fda.gov/apex/f?p=302:26:111381769735406::NO::P26_SERVICE_ID:167
    url18 -> http://intranetappslb.fda.gov/scripts/PasswordRX
    url19 -> https://assetweb.psc.gov/
    url20 -> https://gsaxcess.gov/
    url21 ->
http://sharepoint.fda.gov/orgs/OO-ofems/PPMO/PPMO%20Action%20Tracker/Forms/AllItems.
aspx?InitialTabId=Ribbon%2ELibrary&VisibilityContext=WSSTabPersistence
    url22 -> http://www.opm.gov/healthcare-insurance/dental-vision
    url23 ->
http://www.opm.gov/healthcare-insurance/dental-vision/plan-information/#url=Premiums
    url24 -> http://www.youtube.com/
    url25 -> http://www.adobe.com/
    url26 -> https://itas.hhs.gov/
    url27 -> https://fda.csod.com/
    url28 -> http://go.microsoft.com/fwlink/?LinkId=69157
----------------------------------------
typedurlstime v.20120613
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

TypedURLsTime
Software\Microsoft\Internet Explorer\TypedURLsTime
LastWrite Time Tue Apr 19 20:03:24 2016 (UTC)
    url1 -> Wed Apr 13 14:47:34 2016 Z (http://www.yahoo.com/)
    url2 -> Wed Apr 13 14:47:27 2016 Z (http://www.google.com/)
    url3 -> Tue Apr  5 19:08:51 2016 Z (http://www.gsa.gov/portal/category/22227)
    url4 -> Wed Mar 30 17:15:56 2016 Z (http://tiny.cc/yey49x)
    url5 -> Wed Mar 30 11:18:57 2016 Z (https://faitas.army.mil/Faitas/)
    url6 -> Tue Mar 29 16:47:18 2016 Z
(https://www.surveymonkey.com/r/TALEXApplication)
    url7 -> Tue Mar 22 17:58:59 2016 Z
(https://interact.gsa.gov/user/reset/225010/1458669492/ymSguhZM2qC_5PSHrB6Um_ggg7zS4
BIhkQ8W7u3XOMw)
    url8 -> Fri Mar 18 00:01:43 2016 Z
(http://intranet.fda.gov/omp/smg/guides-manuals.htm)
    url9 -> Wed Mar  9 15:30:30 2016 Z
(http://inside.fda.gov:9003/PolicyProcedures/StaffManualGuide/IssuingStaffManualGuid
es/ucm019808.htm)
    url10 -> Wed Mar  9 13:43:07 2016 Z (http://gsaxcess.gov/fedsweb/pubw2100/)
    url11 -> Wed Feb 10 14:10:17 2016 Z (https://calendar.google.com/calendar)
    url12 -> Wed Jan 20 15:55:11 2016 Z (http://www.gsa.gov/fedfleet)
    url13 -> Tue Jan 19 16:06:11 2016 Z (https://efds.hhs.gov/)
    url14 -> 0
    url15 -> 0
    url16 -> 0
    url17 -> 0
    url18 -> 0
    url19 -> 0
    url20 -> 0
    url21 -> 0
    url22 -> 0
    url23 -> 0
    url24 -> 0
    url25 -> 0

Page 26

Admin OUTPUT.txt

```
    url26 -> 0
    url27 -> 0
    url28 -> 0
-------------------------------------
```
unreadmail v.20100218
(NTUSER.DAT) Gets contents of Unreadmail key

Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
```
-------------------------------------
```
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Run has no values.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Wed Apr 20 15:41:39 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not
found.


Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Apr 20 12:57:39 2016 (UTC)
Run value not found.
run value not found.
load value not found.
```
-------------------------------------
```
user_win v.20080415
(NTUSER.DAT)  --

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Apr 20 12:57:39 2016 (UTC)

```
-------------------------------------
```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Wed Apr 20 16:56:57 2016 Z
    E7CF176E110C211B (7)
Wed Apr 20 16:54:58 2016 Z
    Microsoft.InternetExplorer.Default (1)
Wed Apr 20 16:27:49 2016 Z

Page 27

```
                              Admin OUTPUT.txt
   {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Cisco Systems\Cisco IP
Communicator\communicatork9.exe (2)
Wed Apr 20 15:45:42 2016 Z
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe (1)
Wed Apr 20 15:45:18 2016 Z
   {F38BF404-1D43-42F2-9305-67DE0B28FC23}\explorer.exe (2)
Wed Apr 20 14:54:54 2016 Z
   {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office14\WINWORD.EXE (3)
Wed Apr 20 12:58:58 2016 Z
   {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office14\OUTLOOK.EXE (1)
Wed Apr 20 12:55:53 2016 Z
   Microsoft.Windows.GettingStarted (14)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\displayswitch.exe (13)
   Microsoft.Windows.RemoteDesktop (12)
   Microsoft.Windows.StickyNotes (11)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (10)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (9)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (8)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (7)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe (6)

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Wed Apr 20 16:56:57 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Mozilla Firefox.lnk (5)
Wed Apr 20 16:54:58 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer (3).lnk (1)
Wed Apr 20 16:27:49 2016 Z
   C:\Users\Public\Desktop\Cisco IP Communicator.lnk (2)
Wed Apr 20 15:45:18 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Explorer (3).lnk (2)
Wed Apr 20 15:41:59 2016 Z
   C:\Users\Public\Desktop\Mozilla Firefox.lnk (2)
Wed Apr 20 14:54:54 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Microsoft Word 2010.lnk (3)
Wed Apr 20 12:58:58 2016 Z
   C:\Users\Abe-Arjun.Mallik\Desktop\Microsoft Outlook 2010.lnk (1)
Wed Apr 20 12:55:53 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk (14)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\displayswitch.lnk (13)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk
(12)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (11)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (10)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (9)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (8)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\XPS Viewer.lnk (7)
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk (6)

----------------------------------------
userinfo v.20130513
(NTUSER.DAT) Gets contents of MS Office UserInfo values


Software\Microsoft\Office\Common\UserInfo
LastWrite Time Tue Apr 19 20:03:13 2016 (UTC)
   CompanyName     US FDA
   Company         US FDA
   UserInitials    AAM
   UserName        Mallik, Abe-Arjun

Software\Microsoft\Office\11\.0\Common\UserInfo not found.

----------------------------------------
                              Page 28
```

Admin OUTPUT.txt

userlocsvc v.20090411
(NTUSER.DAT) Displays contents of User Location Service\Client key

Software\Microsoft\User Location Service\Client not found.
------------------------------------
vista_bitbucket v.20080420
(NTUSER.DAT) Get BitBucket settings from Vista via NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Wed Apr 20 12:57:38 2016 (UTC)

LastEnum : 0,{7221dbde-0587-11e6-9667-806e6f6e6963}

{581f0ad3-2ef7-11e5-872a-d4bed95c747d} [Tue Apr 19 20:03:26 2016] (UTC)
    NukeOnDelete      0
{5969b7c2-1dee-11e4-a800-806e6f6e6963} [Tue Apr 19 20:03:26 2016] (UTC)
    NukeOnDelete      0
{7221dbde-0587-11e6-9667-806e6f6e6963} [Wed Apr 20 12:57:38 2016] (UTC)
    NukeOnDelete      0
{d5e2ffea-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2ffeb-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2ffec-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2ffed-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2ffee-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2ffef-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{d5e2fff0-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
{f77e7eee-ae5b-11e5-9806-806e6f6e6963} [Tue Apr 19 20:02:50 2016] (UTC)
    NukeOnDelete      0
------------------------------------
vmplayer v.20110204
(NTUSER.DAT) Extracts full filepath for recent VMware Player VM images.

Software\VMware, Inc.\VMware Player\VMplayer\Window position not found.

------------------------------------
vmware_vsphere_client v.20110204
(NTUSER.DAT) Extract recent connections list for VMware vSphere Client.

Software\VMware\Virtual Infrastructure Client\Preferences\UI\ClientsXml not found.
Software\VMware\VMware Infrastructure Client\Preferences not found.

------------------------------------
vnchookapplicationprefs v.20110208
(NTUSER.DAT) Get VNCHooks Application Prefs list

Software\ORL\VNCHooks\Application_Prefs not found.
------------------------------------
vncviewer v.20121231
(NTUSER.DAT) Get VNCViewer system list

Software\ORL\VNCviewer\MRU not found.
Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------
wallpaper v.200800810
(NTUSER.DAT) Parses Wallpaper MRU Entries

Page 29

Admin OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper\MRU not found.
----------------------------------------
warcraft3 v.20110202
(NTUSER.DAT) Extract usernames for Warcraft 3.

Software\Blizzard Entertainment\Warcraft III\String not found.


----------------------------------------
winlivemail v.20111118
(NTUSER.DAT) Get & display the contents of the Windows Live Mail key

Software\Microsoft\Windows Live Mail not found.
----------------------------------------
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)
   FirstLogon = 0
   ParseAutoexec = 1
   BuildNumber = 7601
   ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
   system had been infected with Bredolab (Symantec).  Also, check the
   contents of a "shell" value - should only include Explorer.exe, if
   it exists.
----------------------------------------
winrar v.20080819
(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.
----------------------------------------
winscp_sessions v.20120809
(NTUSER.DAT) Extracts WinSCP stored session data

"Software\Martin Prikryl\WinSCP 2\Sessions" does not exist
----------------------------------------
winvnc v.20110202
(NTUSER.DAT) Extracts the encrypted password for WinVNC.

Software\ORL\WinVNC3 not found.
Software\ORL\WinVNC3\Default not found.
Software\ORL\WinVNC\Default not found.
Software\RealVNC\WinVNC4 not found.
Software\RealVNC\Default not found.


----------------------------------------
winzip v.20140730
(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.
----------------------------------------
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Wed Apr 20 15:47:37 2016 (UTC)

Searches listed in MRUListEx order

1    .json

Admin OUTPUT.txt

```
0     itunes
---------------------------------------
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

Software\Yahoo\pager not found.
---------------------------------------
```

Page 31

Admin1 OUTPUT.txt

acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
------------------------------------------
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
------------------------------------------
aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install

Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
------------------------------------------
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.

Software\SmartLine Vision\aports not found.

------------------------------------------
appcompatflags v.20130930
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.


------------------------------------------
applets v.20140723
(NTUSER.DAT) Gets contents of user's Applets key

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
------------------------------------------
Software\Microsoft\IntelliPoint\AppSpecific not found.
------------------------------------------
Software\Ares not found.
------------------------------------------
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
------------------------------------------
autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task

Control Panel\Desktop

AutoEndTasks value not found.
------------------------------------------
autorun v.20081212
(NTUSER.DAT) Gets autorun settings

NoDriveTypeAutoRun    0x91
HonorAutorunSetting not found.

Autorun settings in the HKLM hive take precedence over those in
the HKCU hive.
------------------------------------------
bitbucket_user v.20091020
(NTUSER.DAT) TEST - Get user BitBucket values

Page 1

Admin1 OUTPUT.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume
LastWrite Time = Mon Apr 18 16:26:03 2016 (UTC)

------------------------------------
brisv v.20130429
(NTUSER.DAT) Detect artifacts of a Troj.Brisv.A infection

Software\Microsoft\PIMSRV not found.
------------------------------------
cain v.20110204
(NTUSER.DAT) Extracts details for Cain & Abel by oxid.it

Software\Cain\Settings not found.

------------------------------------
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.

------------------------------------
clampi v.20091019
(NTUSER.DAT) TEST - Checks for keys set by Trojan.Clampi PROT module

Software\Microsoft\Internet Explorer\Main
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)


Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete not found.

Software\Microsoft\Internet Account Manager\Accounts not found.

The system does not appear to have been infected with the Trojan.Clampi
PROT module.
------------------------------------
clampitm v.20100624
(NTUSER.DAT) Checks for IOCs for Clampi (per Trend Micro)

ClampiTM plugin
Software\Microsoft\Internet Explorer\Settings
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

No Clampi values found.
------------------------------------
comdlg32 v.20121008

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 not found.
------------------------------------
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted not found.
------------------------------------
compdesc v.20080324
(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions not found.
------------------------------------
controlpanel v.20080428
(NTUSER.DAT) Look for RecentTask* values in ControlPanel key (Vista)

Page 2

Admin1 OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel not found.
-------------------------------------------
cpldontload v.20100116
(NTUSER.DAT) Gets contents of user's Control Panel don't load key

Control Panel\don't load
LastWrite Time Mon Apr 18 16:26:06 2016 (UTC)

Control Panel\don't load has no values.
-------------------------------------------
decaf v.20110210
(NTUSER.DAT) Extracts the EULA value for DECAF.

Software\DECAFme not found.

-------------------------------------------
dependency_walker v.20110204
(NTUSER.DAT) Extracts Recent File List for Dependency Walker.

Software\Microsoft\Dependency Walker\Recent File List not found.

-------------------------------------------
domains v.20100116
(NTUSER.DAT) Gets contents Internet Settings\ZoneMap\Domains key

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap has no subkeys.
-------------------------------------------
environment v.20110204
(NTUSER.DAT) Extracts user's Environment paths from NTUSER.DAT

Environment
Environment
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

TEMP -> %USERPROFILE%\AppData\Local\Temp
TMP -> %USERPROFILE%\AppData\Local\Temp

-------------------------------------------
fileexts v.20080818
(NTUSER.DAT) Get user FileExts values

fileexts
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

-------------------------------------------
filehistory v.20120620
(NTUSER.DAT) Gets filehistory settings

Software\Microsoft\Windows\CurrentVersion\FileHistory not found.
-------------------------------------------
gthist v.20100218
(NTUSER.DAT) Gets Google Toolbar Search History

Software\Google\NavClient\1.1\History not found.
-------------------------------------------
gtwhitelist v.20100218
(NTUSER.DAT) Gets Google Toolbar whitelist values

Software\Google\Google Toolbar\4.0\whitelist not found.
-------------------------------------------
Page 3

Admin1 OUTPUT.txt
haven_and_hearth v.20110204
(NTUSER.DAT) Extracts the username and savedtoken for Haven & Hearth.

Software\JavaSoft\Prefs\haven not found.

------------------------------------------
ie_settings v.20130731
(NTUSER.DAT) Gets important user IE settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)

User Agent = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade = Mon Apr 18 16:26:01 2016 (UTC)
DaysToKeep value not found - default is 20 days

Software\Microsoft\Internet Explorer\Main\WindowsSearch
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
Version = 6.1.7601.17610

'Cleared' value not found.

LastCrawl = Wed Dec 30 13:58:39 2015 UTC
User Favorites Path = file:///C:\Users\Administrator\Favorites\
------------------------------------------
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
   Download Directory = ''

Software\Microsoft\Internet Explorer\AutoComplete not found.

Software\Microsoft\Internet Explorer\DOMStorage
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
Subkeys:
   thehotfixshare.net    ---  Mon Apr 18 16:25:24 2016 UTC
   Total                 ---  Mon Apr 18 16:25:24 2016 UTC

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
   Internet Explorer version = 8.0.7601.19058

Software\Microsoft\Internet Explorer\Main
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
   AllowWindowReuse                        = false [0]
   Anchor Underline                        = yes
   Cache_Update_Frequency                  = Once_Per_Session
   CompatibilityFlags                      = 0 [0x00000000]
   Default_Page_URL                        = http://indside.fda.gov
   Disable Script Debugger                 = yes
   DisableFirstRunCustomize                = 3
   DisableScriptDebuggerIE                 = yes
   Display Inline Images                   = yes
   Do404Search                             = 1 [0x01000000]
   Enable Browser Extensions               = yes
   FullScreen                              = no
   IE8RunOnceLastShown                     = true  [1]
   IE8RunOnceLastShown_TIMESTAMP           = Wed Dec 30 13:01:33 2015 UTC
   IE8RunOncePerInstallCompleted           = true  [1]
   ImageStoreRandomFolder                  = iw9y3oh
   Local Page                              = C:\WINDOWS\system32\blank.htm

Page 4

```
                              Admin1 OUTPUT.txt
    NoUpdateCheck                        = true   [1]
    Play_Animations                      = yes
    Play_Background_Sounds               = yes
    Save_Session_History_On_Exit         = no
    Search Page                          =
http://go.microsoft.com/fwlink/?LinkId=54896
    Show_FullURL                         = no
    Show_StatusBar                       = yes
    Show_ToolBar                         = yes
    Show_URLToolBar                      = yes
    Show_URLinStatusBar                  = yes
    Start Page                           = http://inside.fda.gov:9003/
    UseClearType                         = no
    Use_DlgBox_Colors                    = yes
    Window_Placement                     = <skipped>
    XMLHTTP                              = true   [1]


    Software\Microsoft\Internet Explorer\Main\WindowsSearch
    LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
       ConfiguredScopes        = 4 [0x00000004]
       LastCrawl               = Wed Dec 30 13:58:39 2015 UTC
       User Favorites Path     = file:///C:\Users\Administrator\Favorites\
       Version                 = 6.1.7601.17610

Software\Microsoft\Internet Explorer\Privacy not found (IE should use the default
Privacy settings)

Software\Microsoft\Internet Explorer\Recovery
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

    Software\Microsoft\Internet Explorer\Recovery\Active not found.

    Software\Microsoft\Internet Explorer\Recovery\AdminActive
    LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

    Software\Microsoft\Internet Explorer\Recovery\PendingDelete not found.

Software\Microsoft\Internet Explorer\Suggested Sites
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
    Enabled                   = 0
    LogFileFolder             =
C:\Users\ad_dcc_d.pinckney\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
    ObjectsCreated            = false [0]
    ObjectsCreated_TIMESTAMP  = Wed Dec 30 13:01:45 2015 UTC
    SlicePath                 = C:\Users\Administrator\Favorites\Links\Suggested
Sites.url


-----------------------------------------------
internet_settings_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
    AutoConfigProxy           = wininet.dll
    CertificateRevocation     = true   [1]
    DisableCachingOfSSLPages  = false [0]
    EmailName                 = User@
    EnableHttp1_1             = true   [1]
    EnableNegotiate           = true   [1]
    IE5_UA_Backup_Flag        = 5.0
    MigrateProxy              = true   [1]
    MimeExclusionListForCache = multipart/mixed multipart/x-mixed-replace
                              Page 5
```

```
                                    Admin1 OUTPUT.txt
multipart/x-byteranges
  PrivDiscUiShown                = true  [1]
  PrivacyAdvanced                = false [0]
  ProxyEnable                    = false [0]
  SecureProtocols                = 2688 [0x00000A80]
  UrlEncoding                    = false [0]
  UseSchannelDirectly            = 0x01000000
  User Agent                     = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
  WarnOnIntranet                 = true  [1]
  WarnOnPost                     = 0x01000000
  WarnonZoneCrossing             = false [0]
  ZonesSecurityUpgrade           = Mon Apr 18 16:26:01 2016 UTC


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
    AppContainerContentLimit   = 50
    AppContainerTotalContentLimit = 1000
    ContentLimit               = 250
    Signature                  = Client UrlCache MMF Ver 5.2
    TotalContentLimit          = 0
    Version                    = 1

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
  LastWrite Time Mon Apr 18 16:26:02 2016 (UTC)
    CacheLimit                 = 256000 KB
    CachePrefix                =

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
    CacheLimit                 = 8192 KB
    CachePrefix                = Cookie:

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
    CacheLimit                 = 8192 KB
    CachePrefix                = Visited:


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DOMStore
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
    CacheLimit                 = 1000 KB
    CacheOptions               = 0x8
    CachePath                  = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\DOMStore
    CachePrefix                = DOMStore
    CacheRepair                = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\PrivacIE:
  LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
    CacheLimit                 = 1024 KB
    CacheOptions               = 0x9
    CachePath                  = %APPDATA%\Microsoft\Windows\PrivacIE
    CachePrefix                = PrivacIE:
                                    Page 6
```

```
                              Admin1 OUTPUT.txt
      CacheRepair                 = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\feedplat
     LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x0
      CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Feeds Cache
      CachePrefix                 = feedplat:
      CacheRepair                 = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompat
     LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x9
      CachePath                   = %APPDATA%\Microsoft\Windows\IECompatCache
      CachePrefix                 = iecompat:
      CacheRepair                 = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\ietld
     LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x9
      CachePath                   = %APPDATA%\Microsoft\Windows\IETldCache
      CachePrefix                 = ietld:
      CacheRepair                 = 0x0



   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
   LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)

   subkey 'Extensible Cache' not present


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\CACHE
   LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
      LastScavenge                = true  [1]
      LastScavenge_TIMESTAMP      = Tue Dec 29 19:17:22 2015 UTC
      Persistent                  = 1


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
   LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History
   LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
   ANALYST NOTE:
     No per-domain cookie decisions subkeys are present


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
   LastWrite Time Mon Apr 18 16:26:20 2016 (UTC)

     NETWORK SUBKEY: {51428976-C967-4527-8C08-8643694111E8}
     LastWrite Time Mon Apr 18 16:26:22 2016 (UTC)
        WpadDecision              = 0
        WpadDecisionReason        = 1
        WpadDecisionTime          = Mon Apr 18 16:26:22 2016 UTC
        WpadNetworkName           = fda.gov
        -- MAC SUBKEYS --
        00-1d-45-ac-df-bf           LastWritten Mon Apr 18 16:26:20 2016 UTC
                               Page 7
```

Admin1 OUTPUT.txt

```
NETWORK SUBKEY: {4A85559C-33AC-4EE5-9C05-5EE34C61EE6F}
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
   WpadDecision               = 0
   WpadDecisionReason         = 1
   WpadDecisionTime           = Tue Dec 29 19:16:57 2015 UTC
   WpadNetworkName            = fda.gov
   -- MAC SUBKEYS --
   64-f6-9d-e0-3c-bf             LastWritten Mon Apr 18 16:26:01 2016 UTC


MACs SUBKEY: 64-f6-9d-e0-3c-bf
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
   WpadDecision               = 0
   WpadDecisionReason         = 1
   WpadDecisionTime           = Tue Dec 29 19:16:57 2015 UTC


MACs SUBKEY: 00-1d-45-ac-df-bf
LastWrite Time Mon Apr 18 16:26:22 2016 (UTC)
   WpadDecision               = 0
   WpadDecisionReason         = 1
   WpadDecisionTime           = Mon Apr 18 16:26:22 2016 UTC



 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
  LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
   (default)                 =
   AutoDetect                = 1
   IntranetName              = 0
   ProxyByPass               = 0
   UNCASIntranet             = 0
   -- 'ZoneMap' subkeys -- not parsed:
     Domains               Mon Apr 18 16:25:24 2016 UTC
     EscDomains            Mon Apr 18 16:25:24 2016 UTC
     ProtocolDefaults      Mon Apr 18 16:25:24 2016 UTC
     Ranges                Mon Apr 18 16:25:24 2016 UTC

Subkeys not parsed in 'Software\Microsoft\Windows\CurrentVersion\Internet Settings'

     Activities        ---  Mon Apr 18 16:25:24 2016 UTC
     Connections       ---  Mon Apr 18 16:26:20 2016 UTC
     Http Filters      ---  Mon Apr 18 16:25:24 2016 UTC
     Lockdown_Zones    ---  Mon Apr 18 16:25:24 2016 UTC
     Passport          ---  Mon Apr 18 16:25:24 2016 UTC
     Protocols         ---  Mon Apr 18 16:25:24 2016 UTC
     Zones             ---  Mon Apr 18 16:25:24 2016 UTC

----------------------------------------
javafx v.20110322
(NTUSER.DAT) Gets contents of user's JavaFX key

javafx v.20110322
Software\JavaSoft\Java Update\Policy\JavaFX
LastWrite time: Mon Apr 18 16:31:06 2016

UpdateSchedule            23
UpdateScheduleMinutes     28
Frequency                 8
----------------------------------------
listsoft v.20080324
(NTUSER.DAT) Lists contents of user's Software key

listsoft v.20080324
List the contents of the Software key in the NTUSER.DAT hive
```

Page 8

Admin1 OUTPUT.txt
file, in order by LastWrite time.

```
Mon Apr 18 16:31:06 2016z        JavaSoft
Mon Apr 18 16:27:04 2016z        Adobe
Mon Apr 18 16:26:08 2016z        Microsoft
Mon Apr 18 16:26:05 2016z        Realtek
Mon Apr 18 16:25:58 2016z        NVIDIA Corporation
Mon Apr 18 16:25:44 2016z        Alps
Mon Apr 18 16:25:30 2016z        Intel
Mon Apr 18 16:25:27 2016z        Policies
Mon Apr 18 16:25:24 2016z        AppDataLow
Mon Apr 18 16:25:24 2016z        EMC
Mon Apr 18 16:25:24 2016z        IM Providers
Mon Apr 18 16:25:24 2016z        Wow6432Node
```
----------------------------------------
liveContactsGUID v.20110221
(NTUSER.DAT) Gets user windows Live Messenger GUIDs

Software\Microsoft\Windows Live Contacts\Database not found.
----------------------------------------
load v.20100811
(NTUSER.DAT) Gets load and run values from user hive

load
Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)

load value not found.
run value not found.
----------------------------------------
logonusername v.20080324
(NTUSER.DAT) Get user's Logon User Name value

Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Mon Apr 18 16:37:03 2016 (UTC)]
----------------------------------------
mmc v.20080324
(NTUSER.DAT) Get contents of user's MMC\Recent File List key

MMC - Recent File List
Software\Microsoft\Microsoft Management Console\Recent File List
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
   File1 -> C:\windows\System32\services.msc
----------------------------------------
mndmru v.20080324
(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.
----------------------------------------
mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Remote Drives:
Mon Apr 18 16:25:24 2016 (UTC)
   ##FDSWPCM04264#DeploymentShare$

Volumes:
Mon Apr 18 16:25:24 2016 (UTC)

Page 9

Admin1 OUTPUT.txt
{f77e7eee-ae5b-11e5-9806-806e6f6e6963}
{f77e7ef1-ae5b-11e5-9806-806e6f6e6963}

Drives:
Mon Apr 18 16:25:24 2016 (UTC) - CPC

Unique MAC Addresses:
80:6E:6F:6E:69:63

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices
entries that begin with "\??\Volume".
-----------------------------------------
mpmru v.20080324
(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.
-----------------------------------------
mspaper v.20080324
(NTUSER.DAT) Gets images listed in user's MSPaper key

SOFTWARE\Microsoft\MSPaper* not found.
-----------------------------------------
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
-----------------------------------------
nero v.20100218
(NTUSER.DAT) Gets contents of Ahead\Nero Recent File List subkeys

Software\Ahead not found.
-----------------------------------------
netassist v.20110427
(NTUSER.DAT) Check for Firefox Extensions.

Software\Mozilla\Firefox\Extensions not found.
Software\Microsoft\Windows\CurrentVersion\Uninstall\NetAssistant not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0 not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0\SourceList
not found.

-----------------------------------------
odysseus v.20110202
(NTUSER.DAT) Extract registry keys for Odysseus by bindshell.net.

Software\bindshell.net\Odysseus not found.

-----------------------------------------
officedocs v.20080324
(NTUSER.DAT) Gets contents of user's Office doc MRU keys

officedocs v.20080324
MSOffice version not found.
-----------------------------------------
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version 2010 located.
Software\Microsoft\Office\14.0Word\File MRU not found.

Software\Microsoft\Office\14.0Excel\File MRU not found.

Page 10

Admin1 OUTPUT.txt

Software\Microsoft\Office\14.0\Access\File MRU not found.

Software\Microsoft\Office\14.0\PowerPoint\File MRU not found.
------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

MSOffice version not found.
------------------------------------
OSVersion
Software\Microsoft
LastWrite Time Mon Apr 18 16:26:08 2016 (UTC)

OSVersion value not found.
------------------------------------
outlook v.20100218
(NTUSER.DAT) Gets user's Outlook settings

Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
not found.
------------------------------------
policies_u v.20091021
(NTUSER.DAT) Get values from the user's Policies key


Explorer subkey values:
    NoDriveTypeAutoRun    145
    HideSCAHealth         1
    ForceRunOnStartMenu   1
    NoInplaceSharing      1

System\EnableProfileQuota value not found.
------------------------------------
printermru v.20091125
(NTUSER.DAT) Gets user's Printer Wizard MRU listing

Printers\Settings\Wizard\ConnectMRU not found.
------------------------------------
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Mon Apr 18 16:25:28 2016

    Microsoft XPS Document Writer (winspool,Ne01:,15,45)
    Fax (winspool,Ne01:,15,45)
    Send To OneNote 2010 (winspool,nul:,15,45)
    WebEx Document Loader (winspool,Ne00:,15,45)
    Adobe PDF (winspool,Ne02:,15,45)

Default Printer (via CurrentVersion\Windows): Send To OneNote 2010,winspool,nul:
------------------------------------
privoxy v.20110204
(NTUSER.DAT) Extracts the install path for Privoxy.

Software\Privoxy not found.


------------------------------------
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings

Page 11

```
                            Admin1 OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
    AutoConfigProxy                 wininet.dll
    CertificateRevocation           1
    DisableCachingOfSSLPages        0
    EmailName                       User@
    EnableHttp1_1                   1
    EnableNegotiate                 1
    IE5_UA_Backup_Flag              5.0
    MigrateProxy                    1
    MimeExclusionListForCache       multipart/mixed multipart/x-mixed-replace
multipart/x-byteranges
    PrivDiscUiShown                 1
    PrivacyAdvanced                 0
    ProxyEnable                     0
    SecureProtocols                 2688
    UrlEncoding                     0
    UseSchannelDirectly             1
    User Agent                      Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    WarnOnIntranet                  1
    WarnOnPost                      1
    WarnonZoneCrossing              0
    ZonesSecurityUpgrade            4283908942
----------------------------------------
publishingwizard v.20110202
(NTUSER.DAT) Extract AddNetPlace\LocationMRU for Microsoft Publishing wizard

Software\Microsoft\Windows\CurrentVersion\Explorer\PublishingWizard\AddNetworkPlace\
AddNetPlace\LocationMRU not found.

----------------------------------------
putty v.20110204
(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.

----------------------------------------
rdphint v.20090715
(NTUSER) Gets hosts logged onto via RDP and the Domain\Username

Software\Microsoft\Terminal Server Client\Servers not found.
----------------------------------------
realplayer6 v.20080324
(NTUSER.DAT) Gets user's RealPlayer v6 MostRecentClips(Default) values

Software\RealNetworks\RealPlayer\6.0\Preferences not found.
----------------------------------------
realvnc v.20091125
(NTUSER.DAT) Gets user's RealVNC MRU listing

Software\RealVNC\VNCViewer4\MRU not found.
----------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs has no subkeys.
----------------------------------------
rootkit_revealer v.20110204
                            Page 12
```

Admin1 OUTPUT.txt
(NTUSER.DAT) Extracts the EULA value for Sysinternals Rootkit Revealer.

Software\Sysinternals\RootkitRevealer not found.

------------------------------------------

runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU not found.
------------------------------------------
Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
------------------------------------------
shellfolders v.20090115
(NTUSER.DAT) Retrieve user Shell Folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)
!Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath
function instead
AppData                 C:\Users\ad_dcc_d.pinckney\AppData\Roaming
Local AppData           C:\Users\ad_dcc_d.pinckney\AppData\Local
My Video                C:\Users\ad_dcc_d.pinckney\Videos
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Libraries
My Pictures             C:\Users\ad_dcc_d.pinckney\Pictures
Desktop                 C:\Users\ad_dcc_d.pinckney\Desktop
History
C:\Users\ad_dcc_d.pinckney\AppData\Local\Microsoft\Windows\History
NetHood
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Network Shortcuts
{56784854-C6CB-462B-8169-88E350ACB882} C:\Users\ad_dcc_d.pinckney\Contacts
Cookies
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Cookies
Favorites               C:\Users\ad_dcc_d.pinckney\Favorites
SendTo
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Start Menu
My Music                C:\Users\ad_dcc_d.pinckney\Music
Programs
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Recent
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Recent
CD Burning
C:\Users\ad_dcc_d.pinckney\AppData\Local\Microsoft\Windows\Burn\Burn
PrintHood
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\ad_dcc_d.pinckney\Searches
{374DE290-123F-4565-9164-39C4925E467B} C:\Users\ad_dcc_d.pinckney\Downloads
{A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\ad_dcc_d.pinckney\AppData\LocalLow
Startup
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Administrative Tools
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
Personal                C:\Users\ad_dcc_d.pinckney\Documents
{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\ad_dcc_d.pinckney\Links
Cache
C:\Users\ad_dcc_d.pinckney\AppData\Local\Microsoft\Windows\Temporary Internet Files
Templates
C:\Users\ad_dcc_d.pinckney\AppData\Roaming\Microsoft\Windows\Templates

Page 13

Admin1 OUTPUT.txt
{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\ad_dcc_d.pinckney\Saved Games
Fonts                      C:\WINDOWS\Fonts

------------------------------------------
Software\Skype not found.
------------------------------------------
snapshot_viewer v.20110210
(NTUSER.DAT) Extracts Recent File List for Microsoft Snapshot Viewer.

Software\Microsoft\Snapshot Viewer\Recent File List not found.


------------------------------------------
ssh_host_keys v.20120809
(NTUSER.DAT) Extracts Putty/WinSCP SSH Host Keys

"Software\SimonTatham\Putty\SshHostKeys" does not exist

"Software\Martin Prikryl\WinSCP 2\SshHostKeys" does not exist
------------------------------------------
startmenuinternetapps_cu v.20101219
(NTUSER.DAT) Start Menu Internet Applications info current user

Software\Clients not found. Check the same path in HKLM
------------------------------------------
startpage v.20100330
(NTUSER.DAT) Gets contents of user's StartPage key

Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage
LastWrite Time Mon Apr 18 16:26:04 2016 (UTC)

StartMenu_Start_Time  = Mon Apr 18 16:26:04 2016 Z
StartMenu_Balloon_Time = Wed Dec 30 12:36:56 2015 Z
------------------------------------------
streammru v.20090205
(NTUSER.DAT) streammru

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
------------------------------------------
streams v.20081124
(NTUSER.DAT) Parse Streams and StreamsMRU entries

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
------------------------------------------
Software\SysInternals not found.
------------------------------------------
trustrecords v.20120716
Word

PowerPoint

Excel

Access

------------------------------------------
Launching tsclient v.20120827
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
------------------------------------------
typedpaths v.20100330

Page 14

Admin1 OUTPUT.txt
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
------------------------------------
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
  url1 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
------------------------------------
typedurlstime v.20120613
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

Software\Microsoft\Internet Explorer\TypedURLsTime not found.
------------------------------------
unreadmail v.20100218
(NTUSER.DAT) Gets contents of Unreadmail key

Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Run has no values.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not
found.


Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)
Run value not found.
run value not found.
load value not found.
------------------------------------
user_win v.20080415

Page 15

Admin1 OUTPUT.txt

(NTUSER.DAT)   --

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)

----------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Mon Apr 18 16:26:16 2016 Z
   Microsoft.Windows.MediaPlayer32 (1)
Mon Apr 18 16:24:17 2016 Z
   Microsoft.Windows.GettingStarted (14)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\displayswitch.exe (13)
   Microsoft.Windows.RemoteDesktop (12)
   Microsoft.Windows.StickyNotes (11)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (10)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (9)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (8)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (7)
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe (6)

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Mon Apr 18 16:26:16 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Media Player (3).lnk (1)
Mon Apr 18 16:24:17 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk (14)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\displayswitch.lnk (13)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk
(12)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (11)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (10)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (9)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (8)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\XPS Viewer.lnk (7)
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk (6)

----------------------------------
userinfo v.20130513
(NTUSER.DAT) Gets contents of MS Office UserInfo values


Software\Microsoft\Office\Common\UserInfo
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
   CompanyName      US FDA

Software\Microsoft\Office\11\.0\Common\UserInfo not found.

----------------------------------
userlocsvc v.20090411
(NTUSER.DAT) Displays contents of User Location Service\Client key

Software\Microsoft\User Location Service\Client not found.
----------------------------------
vista_bitbucket v.20080420
(NTUSER.DAT) Get BitBucket settings from Vista via NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Mon Apr 18 16:26:03 2016 (UTC)

LastEnum : 0,{7221dbde-0587-11e6-9667-806e6f6e6963}
                        Page 16

Admin1 OUTPUT.txt

{7221dbde-0587-11e6-9667-806e6f6e6963} [Mon Apr 18 16:26:03 2016] (UTC)
    NukeOnDelete      0
{d5e2ffea-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2ffeb-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2ffec-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2ffed-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2ffee-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2ffef-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{d5e2fff0-f518-11df-a5c1-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
{f77e7eee-ae5b-11e5-9806-806e6f6e6963} [Mon Apr 18 16:25:24 2016] (UTC)
    NukeOnDelete      0
----------------------------------------
vmplayer v.20110204
(NTUSER.DAT) Extracts full filepath for recent VMware Player VM images.

Software\VMware, Inc.\VMware Player\VMplayer\Window position not found.


----------------------------------------
vmware_vsphere_client v.20110204
(NTUSER.DAT) Extract recent connections list for VMware vSphere Client.

Software\VMware\Virtual Infrastructure Client\Preferences\UI\ClientsXml not found.
Software\VMware\VMware Infrastructure Client\Preferences not found.


----------------------------------------
vnchookapplicationprefs v.20110208
(NTUSER.DAT) Get VNCHooks Application Prefs list

Software\ORL\VNCHooks\Application_Prefs not found.
----------------------------------------
vncviewer v.20121231
(NTUSER.DAT) Get VNCViewer system list

Software\ORL\VNCviewer\MRU not found.
Software\RealVNC\VNCViewer4\MRU not found.
----------------------------------------
wallpaper v.200800810
(NTUSER.DAT) Parses Wallpaper MRU Entries

Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper\MRU not found.
----------------------------------------
warcraft3 v.20110202
(NTUSER.DAT) Extract usernames for Warcraft 3.

Software\Blizzard Entertainment\Warcraft III\String not found.


----------------------------------------
winlivemail v.20111118
(NTUSER.DAT) Get & display the contents of the Windows Live Mail key

Software\Microsoft\Windows Live Mail not found.
----------------------------------------
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Page 17

```
                           Admin1 OUTPUT.txt
Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
   FirstLogon = 0
   ParseAutoexec = 1
   BuildNumber = 7601
   ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
   system had been infected with Bredolab (Symantec).  Also, check the
   contents of a "shell" value - should only include Explorer.exe, if
   it exists.
---------------------------------------------
winrar v.20080819
(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.
---------------------------------------------
winscp_sessions v.20120809
(NTUSER.DAT) Extracts WinSCP stored session data

"Software\Martin Prikryl\WinSCP 2\Sessions" does not exist
---------------------------------------------
winvnc v.20110202
(NTUSER.DAT) Extracts the encrypted password for WinVNC.

Software\ORL\WinVNC3 not found.
Software\ORL\WinVNC3\Default not found.
Software\ORL\WinVNC\Default not found.
Software\RealVNC\WinVNC4 not found.
Software\RealVNC\Default not found.


---------------------------------------------
winzip v.20140730
(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.
---------------------------------------------
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Mon Apr 18 16:25:24 2016 (UTC)
Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery has no values.
---------------------------------------------
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

Software\Yahoo\pager not found.
---------------------------------------------
```

Page 18

Admin2 Output.txt

acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
------------------------------------------
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
------------------------------------------
aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install

Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
------------------------------------------
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.

Software\SmartLine Vision\aports not found.

------------------------------------------
appcompatflags v.20130930
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.


Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted
  SIGN.MEDIA=2EF6300 Firefox Setup 45.0.1.exe
  SIGN.MEDIA=2EF6300 ChromeSetup (1).exe
------------------------------------------
applets v.20140723
(NTUSER.DAT) Gets contents of user's Applets key

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
------------------------------------------
Software\Microsoft\IntelliPoint\AppSpecific not found.
------------------------------------------
Software\Ares not found.
------------------------------------------
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
------------------------------------------
autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task

Control Panel\Desktop

AutoEndTasks value not found.
------------------------------------------
autorun v.20081212
(NTUSER.DAT) Gets autorun settings

NoDriveTypeAutoRun    0x91
HonorAutorunSetting not found.

Autorun settings in the HKLM hive take precedence over those in
Page 1

Admin2 Output.txt

the HKCU hive.
----------------------------------------
bitbucket_user v.20091020
(NTUSER.DAT) TEST - Get user BitBucket values

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Tue Apr 19 19:48:43 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume
LastWrite Time = Tue Apr 19 19:48:43 2016 (UTC)

----------------------------------------
brisv v.20130429
(NTUSER.DAT) Detect artifacts of a Troj.Brisv.A infection

Software\Microsoft\PIMSRV not found.
----------------------------------------
cain v.20110204
(NTUSER.DAT) Extracts details for Cain & Abel by oxid.it

Software\Cain\Settings not found.

----------------------------------------
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.

----------------------------------------
clampi v.20091019
(NTUSER.DAT) TEST - Checks for keys set by Trojan.Clampi PROT module

Software\Microsoft\Internet Explorer\Main
LastWrite Time Tue Apr 19 20:45:35 2016 (UTC)


Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete not found.

Software\Microsoft\Internet Account Manager\Accounts not found.

The system does not appear to have been infected with the Trojan.Clampi
PROT module.
----------------------------------------
clampitm v.20100624
(NTUSER.DAT) Checks for IOCs for Clampi (per Trend Micro)

ClampiTM plugin
Software\Microsoft\Internet Explorer\Settings
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

No Clampi values found.
----------------------------------------
comdlg32 v.20121008

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 not found.
----------------------------------------
compatassist
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted
LastWrite Time Tue Apr 19 20:40:22 2016 (UTC)
  SIGN.MEDIA=2EF6300 Firefox Setup 45.0.1.exe
  SIGN.MEDIA=2EF6300 ChromeSetup (1).exe
----------------------------------------
Page 2

Admin2 Output.txt

compdesc v.20080324
(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions not found.
------------------------------------------
controlpanel v.20080428
(NTUSER.DAT) Look for RecentTask* values in ControlPanel key (Vista)

Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel not found.
------------------------------------------
cpldontload v.20100116
(NTUSER.DAT) Gets contents of user's Control Panel don't load key

Control Panel\don't load
LastWrite Time Tue Apr 19 19:48:46 2016 (UTC)

Control Panel\don't load has no values.
------------------------------------------
decaf v.20110210
(NTUSER.DAT) Extracts the EULA value for DECAF.

Software\DECAFme not found.

------------------------------------------
dependency_walker v.20110204
(NTUSER.DAT) Extracts Recent File List for Dependency Walker.

Software\Microsoft\Dependency Walker\Recent File List not found.

------------------------------------------
domains v.20100116
(NTUSER.DAT) Gets contents Internet Settings\ZoneMap\Domains key

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap has no subkeys.
------------------------------------------
environment v.20110204
(NTUSER.DAT) Extracts user's Environment paths from NTUSER.DAT

Environment
Environment
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

TEMP -> %USERPROFILE%\AppData\Local\Temp
TMP -> %USERPROFILE%\AppData\Local\Temp

------------------------------------------
fileexts v.20080818
(NTUSER.DAT) Get user FileExts values

fileexts
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

------------------------------------------
filehistory v.20120620
(NTUSER.DAT) Gets filehistory settings

Software\Microsoft\Windows\CurrentVersion\FileHistory not found.
------------------------------------------
gthist v.20100218
(NTUSER.DAT) Gets Google Toolbar Search History

Page 3

Admin2 Output.txt

Software\Google\NavClient\1.1\History not found.
------------------------------------------
gtwhitelist v.20100218
(NTUSER.DAT) Gets Google Toolbar whitelist values

Software\Google\Google Toolbar\4.0\whitelist not found.
------------------------------------------
haven_and_hearth v.20110204
(NTUSER.DAT) Extracts the username and savedtoken for Haven & Hearth.

Software\JavaSoft\Prefs\haven not found.

------------------------------------------
ie_settings v.20130731
(NTUSER.DAT) Gets important user IE settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)

User Agent = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade = Tue Apr 19 19:48:41 2016 (UTC)
DaysToKeep value not found - default is 20 days

Software\Microsoft\Internet Explorer\Main\WindowsSearch
LastWrite Time Tue Apr 19 20:45:30 2016 (UTC)
Version = 6.1.7601.17610

'Cleared' value not found.

LastCrawl = Wed Dec 30 13:58:39 2015 UTC
UpgradeTime = Tue Apr 19 20:45:30 2016 UTC
User Favorites Path = file:///C:\Users\ad_dcc_s.nchotu\Favorites\
------------------------------------------
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Tue Apr 19 20:45:52 2016 (UTC)
  Download Directory = ''

Software\Microsoft\Internet Explorer\AutoComplete not found.

Software\Microsoft\Internet Explorer\DOMStorage
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
Subkeys:
  thehotfixshare.net    --- Tue Apr 19 19:48:35 2016 UTC
  Total                 --- Tue Apr 19 19:48:35 2016 UTC

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
  Internet Explorer version = 8.0.7601.19058

Software\Microsoft\Internet Explorer\Main
LastWrite Time Tue Apr 19 20:45:35 2016 (UTC)
  AllowWindowReuse                    = false [0]
  Anchor Underline                    = yes
  Cache_Update_Frequency              = Once_Per_Session
  CompatibilityFlags                  = 0 [0x00000000]
  Default_Page_URL                    = http://indside.fda.gov
  Disable Script Debugger             = yes
  DisableFirstRunCustomize            = 3
  DisableScriptDebuggerIE             = yes

Page 4

```
                                    Admin2 Output.txt
    Display Inline Images                = yes
    Do404Search                          = 1 [0x01000000]
    Enable Browser Extensions            = yes
    FullScreen                           = no
    IE10RunOnceCompletionTime            = z'l|Ñ
    IE10RunOncePerInstallCompleted       = 1
    IE8RunOnceLastShown                  = true  [1]
    IE8RunOnceLastShown_TIMESTAMP        = Wed Dec 30 13:01:33 2015 UTC
    IE8RunOncePerInstallCompleted        = true  [1]
    ImageStoreRandomFolder               = iw9y3oh
    Local Page                           = C:\WINDOWS\system32\blank.htm
    NoUpdateCheck                        = true  [1]
    OperationalData                      = |
    Play_Animations                      = yes
    Play_Background_Sounds               = yes
    Save_Session_History_On_Exit         = no
    Search Page                          =
http://go.microsoft.com/fwlink/?LinkId=54896
    Show_FullURL                         = no
    Show_StatusBar                       = yes
    Show_ToolBar                         = yes
    Show_URLToolBar                      = yes
    Show_URLinStatusBar                  = yes
    Start Page                           = http://inside.fda.gov:9003/
    UseClearType                         = no
    Use_DlgBox_Colors                    = yes
    Window_Placement                     = <skipped>
    XMLHTTP                              = true  [1]

Software\Microsoft\Internet Explorer\Main\WindowsSearch
LastWrite Time Tue Apr 19 20:45:30 2016 (UTC)
    ConfiguredScopes         = 5 [0x00000005]
    LastCrawl                = Wed Dec 30 13:58:39 2015 UTC
    UpgradeTime              = Tue Apr 19 20:45:30 2016 UTC
    User Favorites Path      = file:///C:\Users\ad_dcc_s.nchotu\Favorites\
    Version                  = 6.1.7601.17610

Software\Microsoft\Internet Explorer\Privacy not found (IE should use the default
Privacy settings)

Software\Microsoft\Internet Explorer\Recovery
LastWrite Time Tue Apr 19 20:45:28 2016 (UTC)

    Software\Microsoft\Internet Explorer\Recovery\Active not found.

    Software\Microsoft\Internet Explorer\Recovery\AdminActive
    LastWrite Time Tue Apr 19 20:46:05 2016 (UTC)

    Software\Microsoft\Internet Explorer\Recovery\PendingDelete not found.

Software\Microsoft\Internet Explorer\Suggested Sites
LastWrite Time Tue Apr 19 20:45:35 2016 (UTC)
    DataStreamEnabledState       = 0
    Enabled                      = 0
    LogFileFolder                =
C:\Users\ad_dcc_s.nchotu\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
    MigrationTime                = Tue Apr 19 20:45:35 2016 UTC
    ObjectsCreated               = false [0]
    ObjectsCreated_TIMESTAMP     = Wed Dec 30 13:01:45 2015 UTC

------------------------------------------------
internet_settings_cu v.20120528
                                    Page 5
```

```
                              Admin2 Output.txt
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
    AutoConfigProxy                 = wininet.dll
    CertificateRevocation           = true  [1]
    DisableCachingOfSSLPages         = false [0]
    EmailName                       = User@
    EnableHttp1_1                   = true  [1]
    EnableNegotiate                 = true  [1]
    IE5_UA_Backup_Flag              = 5.0
    MigrateProxy                    = true  [1]
    MimeExclusionListForCache       = multipart/mixed multipart/x-mixed-replace
multipart/x-byteranges
    PrivDiscUiShown                 = true  [1]
    PrivacyAdvanced                 = false [0]
    ProxyEnable                     = false [0]
    SecureProtocols                 = 2688 [0x00000A80]
    UrlEncoding                     = false [0]
    UseSchannelDirectly             = 0x01000000
    User Agent                      = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    WarnOnIntranet                  = true  [1]
    WarnOnPost                      = 0x01000000
    WarnonZoneCrossing              = false [0]
    ZonesSecurityUpgrade            = Tue Apr 19 19:48:41 2016 UTC


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
    AppContainerContentLimit   = 50
   ·AppContainerTotalContentLimit = 1000
    ContentLimit               = 250
    Signature                  = Client UrlCache MMF Ver 5.2
    TotalContentLimit          = 0
    Version                    = 1

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
  LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
    CacheLimit                 = 256000 KB
    CachePrefix                =

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
    CacheLimit                 = 8192 KB
    CachePrefix                = Cookie:

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
    CacheLimit                 = 8192 KB
    CachePrefix                = Visited:


    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache
    LastWrite Time Tue Apr 19 20:45:35 2016 (UTC)

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DNTException
    LastWrite Time Tue Apr 19 20:45:28 2016 (UTC)
    CacheLimit                 = 1 KB
                              Page 6
```

```
                                Admin2 Output.txt
CacheOptions              = 0x300
CachePath                 = %APPDATA%\Microsoft\Windows\DNTException
CachePrefix               = DNTException:
CacheRepair               = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DOMStore
   LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
      CacheLimit             = 1000 KB
      CacheOptions           = 0x8
      CachePath              = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\DOMStore
      CachePrefix            = DOMStore
      CacheRepair            = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieBrowserModeList
   LastWrite Time Tue Apr 19 20:45:31 2016 (UTC)
      CacheLimit             = 1 KB
      CacheOptions           = 0x300
      CachePath              = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieBrowserModeList
      CachePrefix            = EmieBrowserModeList:
      CacheRepair            = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieSiteList
   LastWrite Time Tue Apr 19 20:45:31 2016 (UTC)
      CacheLimit             = 1 KB
      CacheOptions           = 0x300
      CachePath              = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieSiteList
      CachePrefix            = EmieSiteList:
      CacheRepair            = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieUserList
   LastWrite Time Tue Apr 19 20:45:31 2016 (UTC)
      CacheLimit             = 1 KB
      CacheOptions           = 0x300
      CachePath              = %USERPROFILE%\AppData\Local\Microsoft\Internet
Explorer\EmieUserList
      CachePrefix            = EmieUserList:
      CacheRepair            = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016041920160420
   LastWrite Time Tue Apr 19 20:45:35 2016 (UTC)
      CacheLimit             = 8192 KB
      CacheOptions           = 0xB
      CachePath              =
%USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016041920
160420
      CachePrefix            = :2016041920160420:
      CacheRepair            = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\PrivacIE:
   LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
      CacheLimit             = 1024 KB
      CacheOptions           = 0x9
      CachePath              = %APPDATA%\Microsoft\Windows\PrivacIE
      CachePrefix            = PrivacIE:
                                Page 7
```

```
                                    Admin2 Output.txt
      CacheRepair                 = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\feedplat
    LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x0
      CachePath                   = %USERPROFILE%\AppData\Local\Microsoft\Feeds Cache
      CachePrefix                 = feedplat:
      CacheRepair                 = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompat
    LastWrite Time Tue Apr 19 20:45:28 2016 (UTC)
      CacheLimit                  = 1 KB
      CacheOptions                = 0x309
      CachePath                   = %APPDATA%\Microsoft\Windows\IECompatCache
      CachePrefix                 = iecompat:
      CacheRepair                 = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompatua
    LastWrite Time Tue Apr 19 20:45:28 2016 (UTC)
      CacheLimit                  = 1 KB
      CacheOptions                = 0x309
      CachePath                   = %APPDATA%\Microsoft\Windows\iecompatuaCache
      CachePrefix                 = iecompatua:
      CacheRepair                 = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iedownload
    LastWrite Time Tue Apr 19 20:45:28 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x9
      CachePath                   = %APPDATA%\Microsoft\Windows\IEDownloadHistory
      CachePrefix                 = iedownload:
      CacheRepair                 = 0x0


  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\ietld
    LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
      CacheLimit                  = 8192 KB
      CacheOptions                = 0x9
      CachePath                   = %APPDATA%\Microsoft\Windows\IETldCache
      CachePrefix                 = ietld:
      CacheRepair                 = 0x0



  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
  LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)

  subkey 'Extensible Cache' not present


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\CACHE
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
      LastScavenge                = true  [1]
      LastScavenge_TIMESTAMP      = Tue Dec 29 19:17:22 2015 UTC
      Persistent                  = 1


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
  LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
                                    Page 8
```

Admin2 Output.txt

Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
ANALYST NOTE:
    No per-domain cookie decisions subkeys are present


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
 LastWrite Time Tue Apr 19 20:55:05 2016 (UTC)

    NETWORK SUBKEY: {51428976-C967-4527-8C08-8643694111E8}
    LastWrite Time Tue Apr 19 20:55:08 2016 (UTC)
        WpadDecision            = 0
        WpadDecisionReason      = 1
        WpadDecisionTime        = Tue Apr 19 20:55:08 2016 UTC
        WpadNetworkName         = fda.gov
        -- MAC SUBKEYS --
        00-08-e3-ff-fc-54       LastWritten Tue Apr 19 20:45:34 2016 UTC
        1c-df-0f-2e-15-7f       LastWritten Tue Apr 19 20:55:05 2016 UTC

    NETWORK SUBKEY: {4A85559C-33AC-4EE5-9C05-5EE34C61EE6F}
    LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
        WpadDecision            = 0
        WpadDecisionReason      = 1
        WpadDecisionTime        = Tue Dec 29 19:16:57 2015 UTC
        WpadNetworkName         = fda.gov
        -- MAC SUBKEYS --
        64-f6-9d-e0-3c-bf       LastWritten Tue Apr 19 19:48:41 2016 UTC

    MACs SUBKEY: 64-f6-9d-e0-3c-bf
    LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
        WpadDecision            = 0
        WpadDecisionReason      = 1
        WpadDecisionTime        = Tue Dec 29 19:16:57 2015 UTC

    MACs SUBKEY: 1c-df-0f-2e-15-7f
    LastWrite Time Tue Apr 19 20:55:08 2016 (UTC)
        WpadDecision            = 0
        WpadDecisionReason      = 1
        WpadDecisionTime        = Tue Apr 19 20:55:08 2016 UTC

    MACs SUBKEY: 00-08-e3-ff-fc-54
    LastWrite Time Tue Apr 19 20:55:08 2016 (UTC)
        WpadDecision            = 0
        WpadDecisionReason      = 1
        WpadDecisionTime        = Tue Apr 19 20:55:08 2016 UTC


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
    (default)               =
    AutoDetect              = 1
    IntranetName            = 0
    ProxyByPass             = 0
    UNCAsIntranet           = 0
    -- 'ZoneMap' subkeys -- not parsed:
        Domains                 Tue Apr 19 19:48:35 2016 UTC
        EscDomains              Tue Apr 19 19:48:35 2016 UTC
        ProtocolDefaults        Tue Apr 19 19:48:35 2016 UTC
        Ranges                  Tue Apr 19 19:48:35 2016 UTC

Subkeys not parsed in 'Software\Microsoft\Windows\CurrentVersion\Internet Settings'

Page 9

```
                              Admin2 Output.txt
    Activities              ---  Tue Apr 19 19:48:35 2016 UTC
    Connections            ---  Tue Apr 19 20:55:08 2016 UTC
    Http Filters           ---  Tue Apr 19 19:48:35 2016 UTC
    Lockdown_Zones         ---  Tue Apr 19 19:48:35 2016 UTC
    Passport               ---  Tue Apr 19 19:48:35 2016 UTC
    Protocols              ---  Tue Apr 19 19:48:35 2016 UTC
    Zones            .     ---  Tue Apr 19 19:48:35 2016 UTC
```
------------------------------------------
javafx v.20110322
(NTUSER.DAT) Gets contents of user's JavaFX key

javafx v.20110322
Software\JavaSoft\Java Update\Policy\JavaFX
LastWrite time: Tue Apr 19 19:53:45 2016

```
UpdateSchedule          0
UpdateScheduleMinutes   28
Frequency               32
```
------------------------------------------
listsoft v.20080324
(NTUSER.DAT) Lists contents of user's Software key

listsoft v.20080324
List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

```
Tue Apr 19 20:55:59 2016Z        Microsoft
Tue Apr 19 20:52:34 2016Z        Cisco Systems, Inc.
Tue Apr 19 20:43:57 2016Z        Mozilla
Tue Apr 19 20:41:20 2016Z        IM Providers
Tue Apr 19 20:41:02 2016Z        Google
Tue Apr 19 20:41:01 2016Z        MozillaPlugins
Tue Apr 19 20:40:52 2016Z        Clients
Tue Apr 19 20:40:41 2016Z        Citrix
Tue Apr 19 19:53:45 2016Z        JavaSoft
Tue Apr 19 19:49:13 2016Z        Alps
Tue Apr 19 19:48:47 2016Z        Adobe
Tue Apr 19 19:48:47 2016Z        McAfee
Tue Apr 19 19:48:46 2016Z        NVIDIA Corporation
Tue Apr 19 19:48:45 2016Z        Realtek
Tue Apr 19 19:48:41 2016Z        FDA
Tue Apr 19 19:48:39 2016Z        KiXtart
Tue Apr 19 19:48:37 2016Z        Intel
Tue Apr 19 19:48:35 2016Z        AppDataLow
Tue Apr 19 19:48:35 2016Z        EMC
Tue Apr 19 19:48:35 2016Z        Policies
Tue Apr 19 19:48:35 2016Z        Wow6432Node
```
------------------------------------------
liveContactsGUID v.20110221
(NTUSER.DAT) Gets user Windows Live Messenger GUIDs

Software\Microsoft\Windows Live Contacts\Database not found.
------------------------------------------
load v.20100811
(NTUSER.DAT) Gets load and run values from user hive

load
Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Tue Apr 19 19:48:46 2016 (UTC)

load value not found.
run value not found.

Page 10

Admin2 Output.txt
------------------------------------------
logonusername v.20080324
(NTUSER.DAT) Get user's Logon User Name value

Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Tue Apr 19 20:56:38 2016 (UTC)]
------------------------------------------
mmc v.20080324
(NTUSER.DAT) Get contents of user's MMC\Recent File List key

MMC - Recent File List
Software\Microsoft\Microsoft Management Console\Recent File List
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
   File1 -> C:\windows\System32\services.msc
------------------------------------------
mndmru v.20080324
(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.
------------------------------------------
mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Tue Apr 19 20:37:37 2016 (UTC)

Remote Drives:
Tue Apr 19 19:48:35 2016 (UTC)
   ##FDSWPCM04264#DeploymentShare$

Volumes:
Tue Apr 19 20:53:18 2016 (UTC)
   {8fc79a65-0667-11e6-8233-34e6d733e6f7}
Tue Apr 19 19:48:35 2016 (UTC)
   {f77e7eee-ae5b-11e5-9806-806e6f6e6963}
   {f77e7ef1-ae5b-11e5-9806-806e6f6e6963}

Drives:
Tue Apr 19 19:48:35 2016 (UTC) - CPC

Unique MAC Addresses:
80:6E:6F:6E:69:63
34:E6:D7:33:E6:F7

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices
entries that begin with "\??\Volume".
------------------------------------------
mpmru v.20080324
(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.
------------------------------------------
mspaper v.20080324
(NTUSER.DAT) Gets images listed in user's MSPaper key

SOFTWARE\Microsoft\MSPaper* not found.
------------------------------------------
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.
                          Page 11

Admin2 Output.txt

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
-----------------------------------------
nero v.20100218
(NTUSER.DAT) Gets contents of Ahead\Nero Recent File List subkeys

Software\Ahead not found.
-----------------------------------------
netassist v.20110427
(NTUSER.DAT) Check for Firefox Extensions.

Software\Mozilla\Firefox\Extensions not found.
Software\Microsoft\Windows\CurrentVersion\Uninstall\NetAssistant not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0 not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0\SourceList
not found.

-----------------------------------------
odysseus v.20110202
(NTUSER.DAT) Extract registry keys for Odysseus by bindshell.net.

Software\bindshell.net\Odysseus not found.

-----------------------------------------
officedocs v.20080324
(NTUSER.DAT) Gets contents of user's Office doc MRU keys

officedocs v.20080324
MSOffice version not found.
-----------------------------------------
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version 2010 located.
Software\Microsoft\Office\14.0Word\File MRU not found.

Software\Microsoft\Office\14.0Excel\File MRU not found.

Software\Microsoft\Office\14.0\Access\File MRU not found.

Software\Microsoft\Office\14.0\PowerPoint\File MRU not found.
-----------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

MSOffice version not found.
-----------------------------------------
OSVersion
Software\Microsoft
LastWrite Time Tue Apr 19 20:55:59 2016 (UTC)

OSVersion value not found.
-----------------------------------------
outlook v.20100218
(NTUSER.DAT) Gets user's Outlook settings

Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
not found.
-----------------------------------------
policies_u v.20091021
(NTUSER.DAT) Get values from the user's Policies key

Page 12

Admin2 Output.txt

Explorer subkey values:
  NoDriveTypeAutoRun    145
  HideSCAHealth        1
  ForceRunOnStartMenu  1

System\EnableProfileQuota value not found.
----------------------------------------
printermru v.20091125
(NTUSER.DAT) Gets user's Printer Wizard MRU listing

Printers\Settings\Wizard\ConnectMRU not found.
----------------------------------------
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Tue Apr 19 19:48:46 2016

  Microsoft XPS Document Writer (winspool,Ne01:,15,45)
  Fax (winspool,Ne01:,15,45)
  Send To OneNote 2010 (winspool,nul:,15,45)
  WebEx Document Loader (winspool,Ne00:,15,45)
  Adobe PDF (winspool,Ne02:,15,45)

Default Printer (via CurrentVersion\Windows): Send To OneNote 2010,winspool,nul:
----------------------------------------
privoxy v.20110204
(NTUSER.DAT) Extracts the install path for Privoxy.

Software\Privoxy not found.

----------------------------------------
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
  AutoConfigProxy              wininet.dll
  CertificateRevocation       1
  DisableCachingOfSSLPages    0
  EmailName               User@
  EnableHttp1_1           1
  EnableNegotiate         1
  IE5_UA_Backup_Flag      5.0
  MigrateProxy            1
  MimeExclusionListForCache   multipart/mixed multipart/x-mixed-replace
multipart/x-byteranges
  PrivDiscUIShown         1
  PrivacyAdvanced         0
  ProxyEnable             0
  SecureProtocols         2688
  UrlEncoding             0
  UseSchannelDirectly     1
  User Agent             Mozilla/4.0 (compatible; MSIE 8.0; Win32)
  WarnOnIntranet         1
  WarnOnPost              1
  WarnonZoneCrossing      0
  ZonesSecurityUpgrade    2039502029
----------------------------------------
publishingwizard v.20110202
(NTUSER.DAT) Extract AddNetPlace\LocationMRU for Microsoft Publishing Wizard

Page 13

Admin2 Output.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\PublishingWizard\AddNetworkPlace\
AddNetPlace\LocationMRU not found.

------------------------------------
putty v.20110204
(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.

------------------------------------
rdphint v.20090715
(NTUSER) Gets hosts logged onto via RDP and the Domain\Username

Software\Microsoft\Terminal Server Client\Servers not found.
------------------------------------
realplayer6 v.20080324
(NTUSER.DAT) Gets user's RealPlayer v6 MostRecentClips(Default) values

Software\RealNetworks\RealPlayer\6.0\Preferences not found.
------------------------------------
realvnc v.20091125
(NTUSER.DAT) Gets user's RealVNC MRU listing

Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs has no subkeys.
------------------------------------
rootkit_revealer v.20110204
(NTUSER.DAT) Extracts the EULA value for Sysinternals Rootkit Revealer.

Software\Sysinternals\RootkitRevealer not found.

------------------------------------
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Tue Apr 19 20:44:12 2016 (UTC)
MRUList = a
a    \\fda\wodc\OC\1
------------------------------------
Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
------------------------------------
shellfolders v.20090115
(NTUSER.DAT) Retrieve user Shell Folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
LastWrite Time Tue Apr 19 19:48:43 2016 (UTC)
!Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath
function instead
AppData              C:\Users\ad_dcc_s.nchotu\AppData\Roaming
Local AppData        C:\Users\ad_dcc_s.nchotu\AppData\Local
My Video             C:\Users\ad_dcc_s.nchotu\Videos
Page 14

Admin2 Output.txt
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Libraries
My Pictures            C:\Users\ad_dcc_s.nchotu\Pictures
Desktop                C:\Users\ad_dcc_s.nchotu\Desktop
History
C:\Users\ad_dcc_s.nchotu\AppData\Local\Microsoft\Windows\History
NetHood
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Network Shortcuts
{56784854-C6CB-462B-8169-88E350ACB882} C:\Users\ad_dcc_s.nchotu\Contacts
Cookies
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Cookies
Favorites              C:\Users\ad_dcc_s.nchotu\Favorites
SendTo
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Start Menu
My Music               C:\Users\ad_dcc_s.nchotu\Music
Programs
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Recent
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Recent
CD Burning
C:\Users\ad_dcc_s.nchotu\AppData\Local\Microsoft\Windows\Burn\Burn
PrintHood
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\ad_dcc_s.nchotu\Searches
{374DE290-123F-4565-9164-39C4925E467B} C:\Users\ad_dcc_s.nchotu\Downloads
{A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\ad_dcc_s.nchotu\AppData\LocalLow
Startup
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Administrative Tools
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Start
·Menu\Programs\Administrative Tools
Personal               C:\Users\ad_dcc_s.nchotu\Documents
{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\ad_dcc_s.nchotu\Links
Cache
C:\Users\ad_dcc_s.nchotu\AppData\Local\Microsoft\Windows\Temporary Internet Files
Templates
C:\Users\ad_dcc_s.nchotu\AppData\Roaming\Microsoft\Windows\Templates
{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\ad_dcc_s.nchotu\Saved Games
Fonts                  C:\WINDOWS\Fonts

------------------------------------------
Software\Skype not found.
------------------------------------------
snapshot_viewer v.20110210
(NTUSER.DAT) Extracts Recent File List for Microsoft Snapshot Viewer.

Software\Microsoft\Snapshot Viewer\Recent File List not found.

------------------------------------------
ssh_host_keys v.20120809
(NTUSER.DAT) Extracts Putty/WinSCP SSH Host Keys

"Software\SimonTatham\Putty\SshHostKeys" does not exist

"Software\Martin Prikryl\WinSCP 2\SshHostKeys" does not exist
------------------------------------------
startmenuinternetapps_cu v.20101219
(NTUSER.DAT) Start Menu Internet Applications info current user

Start Menu Internet Applications
                              Page 15

Admin2 Output.txt

StartMenuInternet [Tue Apr 19 20:40:52 2016 (UTC)]
NOTE: default Internet Browser client key
(default) -> FIREFOX.EXE

-------------------------------------------
startpage v.20100330
(NTUSER.DAT) Gets contents of user's StartPage key

Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage
LastWrite Time Tue Apr 19 20:56:11 2016 (UTC)

StartMenu_Start_Time   = Tue Apr 19 19:48:44 2016 Z
StartMenu_Balloon_Time = Wed Dec 30 12:36:56 2015 Z
-------------------------------------------
streammru v.20090205
(NTUSER.DAT) streammru

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
-------------------------------------------
streams v.20081124
(NTUSER.DAT) Parse Streams and StreamsMRU entries

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
-------------------------------------------
Software\SysInternals not found.
-------------------------------------------
trustrecords v.20120716
Word

PowerPoint

Excel

Access

-------------------------------------------
Launching tsclient v.20120827
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
-------------------------------------------
typedpaths v.20100330
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
-------------------------------------------
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Tue Apr 19 19:48:41 2016 (UTC)
   url1 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
-------------------------------------------
typedurlstime v.20120613
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

Page 16

Admin2 Output.txt

Software\Microsoft\Internet Explorer\TypedURLsTime not found.
----------------------------------------
unreadmail v.20100218
(NTUSER.DAT) Gets contents of Unreadmail key

Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
----------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Run has no values.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not
found.


Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Tue Apr 19 19:48:46 2016 (UTC)
Run value not found.
run value not found.
load value not found.
----------------------------------------
user_win v.20080415
(NTUSER.DAT)  --

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Tue Apr 19 19:48:46 2016 (UTC)


----------------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Tue Apr 19 20:54:51 2016 Z
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msiexec.exe (4)
Tue Apr 19 20:52:34 2016 Z
   {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Cisco Systems\Cisco IP
Communicator\communicatork9.exe (1)
Tue Apr 19 20:52:31 2016 Z
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (1)
Page 17

```
                              Admin2 Output.txt
Tue Apr 19 20:40:38 2016 Z
  D:\GoToMeeting Codec\g2m_codec.exe (1)
Tue Apr 19 20:40:17 2016 Z
  D:\Firefox Setup 45.0.1.exe (1)
Tue Apr 19 20:40:05 2016 Z
  D:\ChromeSetup (1).exe (1)
Tue Apr 19 19:49:31 2016 Z
  C:\Users\ad_dcc_s.nchotu\Desktop\Launch_PCRestore.exe (1)
Tue Apr 19 19:46:57 2016 Z
  Microsoft.Windows.GettingStarted (14)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\displayswitch.exe (13)
  Microsoft.Windows.RemoteDesktop (12)
  Microsoft.Windows.StickyNotes (11)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (9)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (7)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe (6)

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Tue Apr 19 20:52:34 2016 Z
  C:\Users\Public\Desktop\Cisco IP Communicator.lnk (1)
Tue Apr 19 19:46:57 2016 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk (14)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\displayswitch.lnk (13)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk
(12)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (11)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (10)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (9)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (8)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\XPS Viewer.lnk (7)
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk (6)


----------------------------------------
userinfo v.20130513
(NTUSER.DAT) Gets contents of MS Office UserInfo values


Software\Microsoft\Office\Common\UserInfo
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
  CompanyName     US FDA

Software\Microsoft\Office\11\.0\Common\UserInfo not found.

----------------------------------------
userlocsvc v.20090411
(NTUSER.DAT) Displays contents of User Location Service\Client key

Software\Microsoft\User Location Service\Client not found.
----------------------------------------
vista_bitbucket v.20080420
(NTUSER.DAT) Get BitBucket settings from Vista via NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Tue Apr 19 19:48:43 2016 (UTC)

LastEnum : 0,{7221dbde-0587-11e6-9667-806e6f6e6963}

{7221dbde-0587-11e6-9667-806e6f6e6963} [Tue Apr 19 20:56:11 2016] (UTC)
  NukeOnDelete     0
{d5e2ffea-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
  NukeOnDelete     0
```

*₁*

```
                                    Admin2 Output.txt
{d5e2ffeb-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{d5e2ffec-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{d5e2ffed-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{d5e2ffee-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{d5e2ffef-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{d5e2fff0-f518-11df-a5c1-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
{f77e7eee-ae5b-11e5-9806-806e6f6e6963} [Tue Apr 19 19:48:35 2016] (UTC)
   NukeOnDelete      0
-------------------------------------
vmplayer v.20110204
(NTUSER.DAT) Extracts full filepath for recent VMware Player VM images.

Software\VMware, Inc.\VMware Player\VMplayer\Window position not found.


-------------------------------------
vmware_vsphere_client v.20110204
(NTUSER.DAT) Extract recent connections list for VMware vSphere Client.

Software\VMware\Virtual Infrastructure Client\Preferences\UI\ClientsXml not found.
Software\VMware\VMware Infrastructure Client\Preferences not found.


-------------------------------------
vnchookapplicationprefs v.20110208
(NTUSER.DAT) Get VNCHooks Application Prefs list

Software\ORL\VNCHooks\Application_Prefs not found.
-------------------------------------
vncviewer v.20121231
(NTUSER.DAT) Get VNCViewer system list

Software\ORL\VNCViewer\MRU not found.
Software\RealVNC\VNCViewer4\MRU not found.
-------------------------------------
wallpaper v.200800810
(NTUSER.DAT) Parses Wallpaper MRU Entries

Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper\MRU not found.
-------------------------------------
warcraft3 v.20110202
(NTUSER.DAT) Extract usernames for Warcraft 3.

Software\Blizzard Entertainment\Warcraft III\String not found.


-------------------------------------
winlivemail v.20111118
(NTUSER.DAT) Get & display the contents of the Windows Live Mail key

Software\Microsoft\Windows Live Mail not found.
-------------------------------------
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
   FirstLogon = 0
   ParseAutoexec = 1
   BuildNumber = 7601
                                    Page 19
```

Admin2 Output.txt
ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
    system had been infected with Bredolab (Symantec).  Also, check the
    contents of a "shell" value - should only include Explorer.exe, if
    it exists.
----------------------------------------
winrar v.20080819
(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.
----------------------------------------
winscp_sessions v.20120809
(NTUSER.DAT) Extracts WinSCP stored session data

"Software\Martin Prikryl\WinSCP 2\Sessions" does not exist
----------------------------------------
winvnc v.20110202
(NTUSER.DAT) Extracts the encrypted password for WinVNC.

Software\ORL\WinVNC3 not found.
Software\ORL\WinVNC3\Default not found.
Software\ORL\WinVNC\Default not found.
Software\RealVNC\WinVNC4 not found.
Software\RealVNC\Default not found.


----------------------------------------
winzip v.20140730
(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.
----------------------------------------
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Tue Apr 19 19:48:35 2016 (UTC)
Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery has no values.
----------------------------------------
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

Software\Yahoo\pager not found.
----------------------------------------

Page 20

```
                        SAM OUTPUT.txt
samparse v.20120722
(SAM) Parse SAM file for user & group mbrshp info


User Information
------------------------
Username        : ScottC [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Mon Apr 18 16:17:34 2016 Z
Last Login Date : Wed Dec 30 13:52:20 2015 Z
Pwd Reset Date  : Mon Apr 18 15:29:26 2016 Z
Pwd Fail Date   : Never
Login Count     : 18
   --> Password does not expire
   --> Account Disabled
   --> Normal user account


Username        : RogerS [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Mon Apr 18 16:17:34 2016 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
   --> Password does not expire
   --> Account Disabled
   --> Password not required
   --> Normal user account


Username        : SidneyR [1000]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Tue Dec 29 15:49:10 2015 Z
Last Login Date : Never
Pwd Reset Date  : Wed Apr 20 15:26:28 2016 Z
Pwd Fail Date   : Never
Login Count     : 0
   --> Password does not expire
   --> Normal user account


------------------------
Group Membership Information
------------------------
Group Name    : Users [4]
LastWrite     : Mon Apr 18 15:29:03 2016 Z
Group Comment : Users are prevented from making accidental or intentional
system-wide changes and can run most applications
Users :
   S-1-5-4
   S-1-5-11
   S-1-5-21-1078081533-606747145-839522115-513
   S-1-5-21-2431487851-277683799-2983902431-1000

Group Name    : Event Log Readers [0]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Members of this group can read event logs from local machine
Users         : None


                        Page 1
```

SAM OUTPUT.txt
```
Group Name     : Guests [1]
LastWrite      : Mon Apr 18 15:26:52 2016 Z
Group Comment  : Guests have the same access as members of the Users group by
default, except for the Guest account which is further restricted
Users :
   S-1-5-21-2431487851-277683799-2983902431-501

Group Name     : Distributed COM Users [0]
LastWrite      : Tue Jul 14 04:45:47 2009 Z
Group Comment  : Members are allowed to launch, activate and use Distributed COM
objects on this machine.
Users          : None

Group Name     : Administrators [5]
LastWrite      : Tue Apr 19 20:04:08 2016 Z
Group Comment  : Administrators have complete and unrestricted access to the
computer/domain
Users :
   S-1-5-21-1078081533-606747145-839522115-27710
   S-1-5-21-2431487851-277683799-2983902431-500
   S-1-5-21-2431487851-277683799-2983902431-1000
   S-1-5-21-1078081533-606747145-839522115-27712
   S-1-5-21-1078081533-606747145-839522115-512

Group Name     : Network Configuration Operators [0]
LastWrite      : Tue Dec 29 18:43:49 2015 Z
Group Comment  : Members in this group can have some administrative privileges to
manage configuration of networking features
Users          : None

Group Name     : Cryptographic Operators [0]
LastWrite      : Tue Dec 29 18:43:49 2015 Z
Group Comment  : Members are authorized to perform cryptographic operations.
Users          : None

Group Name     : Power Users [0]
LastWrite      : Tue Dec 29 18:43:49 2015 Z
Group Comment  : Power Users are included for backwards compatibility and possess
limited administrative powers
Users          : None

Group Name     : Performance Log Users [0]
LastWrite      : Tue Jul 14 04:45:46 2009 Z
Group Comment  : Members of this group may schedule logging of performance counters,
enable trace providers, and collect event traces both locally and via remote access
to this computer
Users          : None

Group Name     : Replicator [0]
LastWrite      : Tue Dec 29 18:43:49 2015 Z
Group Comment  : Supports file replication in a domain
Users          : None

Group Name     : Performance Monitor Users [0]
LastWrite      : Tue Jul 14 04:45:46 2009 Z
Group Comment  : Members of this group can access performance counter data locally
and remotely
Users          : None

Group Name     : Remote Desktop Users [0]
LastWrite      : Tue Dec 29 18:43:49 2015 Z
Group Comment  : Members in this group are granted the right to logon remotely
Users          : None
```
Page 2

SAM OUTPUT.txt

```
Group Name      : IIS_IUSRS [1]
LastWrite       : Tue Jul 14 04:45:47 2009 Z
Group Comment   : Built-in group used by Internet Information Services.
Users :
  S-1-5-17

Group Name      : Backup Operators [0]
LastWrite       : Tue Dec 29 18:43:49 2015 Z
Group Comment   : Backup Operators can override security restrictions for the sole
purpose of backing up or restoring files
Users           : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
      - S-1-5-4  = Interactive
      - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin
```

----------------------------------------

Page 3

SECURITY OUTPUT.txt

auditpol v.20121128
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time Mon Apr 18 16:17:35 2016 (UTC)

Length of data: 138 bytes.
```
0x00000000: 00 01 00 00 09 00 00 00 78 00 00 00 03 00 03 00   ........x.......
0x00000010: 03 00 03 00 00 00 03 00 01 00 00 00 00 00 01 00   ................
0x00000020: 00 00 00 00 00 00 00 00 02 00 02 00 00 00 00 00   ................
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000040: 03 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00   ................
0x00000050: 01 00 00 00 00 00 00 00 00 00 03 00 03 00 03 00   ................
0x00000060: 00 00 00 00 03 00 00 00 00 00 00 00 00 00 03 00   ................
0x00000070: 00 00 00 00 00 00 00 00 05 00 09 00 0c 00 03 00   ................
0x00000080: 04 00 06 00 06 00 04 00 04 00                     ..........
```
**Auditing is NOT enabled.
----------------------------------------
lsasecrets v.20140408
(Security) TEST - Get update times for LSA Secrets

Domain secret - $MACHINE.ACC
CupdTime = Mon Apr 18 15:29:03 2016
OupdTime = Mon Apr 18 15:29:03 2016
----------------------------------------
polacdms v.20100531
(Security) Get local machine SID from Security hive

PolAcDmS
Policy\PolAcDmS
LastWrite Time Mon Apr 18 15:26:52 2016 (UTC)

Machine SID: S-1-5-21-2431487851-277683799-2983902431

PolPrDmS
Policy\PolPrDmS
LastWrite Time Mon Apr 18 15:29:03 2016 (UTC)

Primary Domain SID: S-1-5-21-1078081533-606747145-839522115
----------------------------------------

Page 1

SOFTWARE OUTPUT.txt
Launching appinitdlls v.20130425
appinitdlls v.20130425
(Software) Gets contents of AppInit_DLLs value

AppInit_DLLs
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Mon Apr 18 15:30:11 2016 (UTC)
   AppInit_DLLs : C:\WINDOWS\system32\nvinitx.dll
   LoadAppInit_DLLs : 1
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Mon Apr 18 15:30:11 2016 (UTC)
   AppInit_DLLs : C:\WINDOWS\SysWOW64\nvinit.dll
   LoadAppInit_DLLs : 1
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
----------------------------------------------
apppaths v.20120524
(Software) Gets content of App Paths subkeys

App Paths
Microsoft\Windows\CurrentVersion\App Paths

Tue Apr 19 20:41:00 2016 (UTC)
   chrome.exe - C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Tue Apr 19 20:40:52 2016 (UTC)
   firefox.exe - C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Tue Apr 19 20:40:19 2016 (UTC)
   communicatorK9.exe - C:\Program Files (x86)\Cisco Systems\Cisco IP
Communicator\communicatorK9.exe
Mon Apr 18 15:54:27 2016 (UTC)
   javaws.exe - C:\progra~2\java\jre-1.6.38\bin\javaws.exe
Mon Apr 18 15:53:53 2016 (UTC)
   javaw.Exe - C:\Program Files (x86)\Oracle\JInitiator 1.3.1.26\bin\javaw.Exe
Mon Apr 18 15:50:45 2016 (UTC)
   IEDIAG.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
   IEDIAGCMD.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
   IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
Mon Apr 18 15:45:53 2016 (UTC)
   winzip.exe - C:\Program Files\WinZip\winzip64.exe
   winzip32.exe - C:\Program Files\WinZip\winzip64.exe
Mon Apr 18 15:45:43 2016 (UTC)
   winzip64.exe - C:\Program Files\WinZip\winzip64.exe
Mon Apr 18 15:44:18 2016 (UTC)
   Acrobat.exe - C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Acrobat.exe
   AcrobatInfo.exe - C:\Program Files (x86)\Adobe\Acrobat
10.0\Acrobat\AcrobatInfo.exe
   AcroDist.exe - C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\AcroDist.exe
Mon Apr 18 15:28:51 2016 (UTC)
   fsquirt.exe -
Wed Dec 30 12:20:19 2015 (UTC)
   ERClient7.exe - C:\Program Files (x86)\eRoom 7\ERClient7.exe
Tue Dec 29 19:03:59 2015 (UTC)
   msoxmled.exe - C:\Program Files (x86)\Common Files\Microsoft
Shared\OFFICE14\MSOXMLED.EXE
Tue Dec 29 18:43:51 2015 (UTC)
   vstoee.dll -
Tue Dec 29 18:43:08 2015 (UTC)
                              Page 1

SOFTWARE OUTPUT.txt
```
    cmmgr32.exe -
Tue Dec 29 16:07:32 2015 (UTC)
    communicator.exe - C:\Program Files (x86)\Microsoft Lync\communicator.exe
Tue Dec 29 15:55:13 2015 (UTC)
   MSPUB.EXE - C:\PROGRA~2\MICROS~1\Office14\MSPUB.EXE
   powerpnt.exe - C:\PROGRA~2\MICROS~1\Office14\POWERPNT.EXE
   Winword.exe - C:\PROGRA~2\MICROS~1\Office14\WINWORD.EXE
Tue Dec 29 15:55:12 2015 (UTC)
   excel.exe - C:\PROGRA~2\MICROS~1\Office14\EXCEL.EXE
   GROOVE.EXE - C:\PROGRA~2\MICROS~1\Office14\GROOVE.EXE
   MSACCESS.EXE - C:\PROGRA~2\MICROS~1\Office14\MSACCESS.EXE
   OneNote.exe - C:\PROGRA~2\MICROS~1\Office14\ONENOTE.EXE
   OUTLOOK.EXE - C:\PROGRA~2\MICROS~1\Office14\OUTLOOK.EXE
Tue Dec 29 15:55:11 2015 (UTC)
   ois.exe - C:\PROGRA~2\MICROS~1\office14\OIS.EXE
Tue Dec 29 15:52:10 2015 (UTC)
   MsoHtmEd.exe -
Tue Apr 12 07:45:35 2011 (UTC)
   mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe
Tue Apr 12 07:45:34 2011 (UTC)
   dvdmaker.exe - %ProgramFiles%\DVD Maker\dvdmaker.exe
   Journal.exe - %ProgramFiles%\Windows Journal\Journal.exe
   SnippingTool.exe - %SystemRoot%\system32\SnippingTool.exe
   TabTip.exe - %CommonProgramFiles%\microsoft shared\ink\TabTip.exe
Tue Jul 14 04:53:25 2009 (UTC)
   install.exe -
   migwiz.exe -
   mplayer2.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
   pbrush.exe - %SystemRoot%\System32\mspaint.exe
   PowerShell.exe - %SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe
   setup.exe -
   sidebar.exe - "%ProgramFiles%\Windows Sidebar\sidebar.exe"
   table30.exe -
   wab.exe - %ProgramFiles%\Windows Mail\wab.exe
   wabmig.exe - %ProgramFiles%\Windows Mail\wabmig.exe
   wmplayer.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
   WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
   WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths not found.
-------------------------------------
assoc v.20080815
(Software) Get list of file ext associations

assoc
Classes

-------------------------------------
banner v.20081119
(Software) Get HKLM\SOFTWARE.. Logon Banner Values

Logon Banner Information
Microsoft\Windows\CurrentVersion\policies\system
LastWrite Time Wed Apr 20 15:41:10 2016 (UTC)

Legalnoticecaption value = Warning **** Warning **** Warning

Legalnoticetext value = You are accessing a U.S. Government information system,
which includes (1) this computer, (2) this computer network, (3) all computers
connected to this network, and (4) all devices and storage media attached to this
network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only.
Unauthorized or improper use of this system may result in disciplinary action, as
```
Page 2

SOFTWARE OUTPUT.txt
well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

• You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

• Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Wed Apr 20 15:40:55 2016 (UTC)

Legalnoticecaption value =

Legalnoticetext value =

------------------------------------------
bho v.20130408
(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
LastWrite Time Mon Apr 18 15:58:30 2016 (UTC)

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}
    Class      => Groove GFS Browser Helper
    Module     => C:\PROGRA~1\MICROS~1\Office14\GROOVEEX.DLL
    LastWrite => Tue Dec 29 15:52:07 2015

{7DB2D5A0-7241-4E79-B68D-6309F01C5231}
    Class      => scriptproxy
    Module     => C:\Program Files\Common
Files\McAfee\SystemCore\ScriptSn.20160418115830.dll
    LastWrite => Mon Apr 18 15:58:30 2016

{90E2BA2E-DD1B-4cde-9134-7A8B86D33CA7}
    Class      => WebEx Productivity Tools
    Module     => C:\Program Files (x86)\WebEx\Productivity Tools\ptonecli64.dll
    LastWrite => Mon Apr 18 15:54:54 2016

{B4F3A835-0E21-4959-BA22-42B3008E02FF}
    Class      => Office Document Cache Handler
    Module     => C:\PROGRA~1\MICROS~1\Office14\URLREDIR.DLL
    LastWrite => Tue Dec 29 15:52:07 2015

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
LastWrite Time Mon Apr 18 15:58:31 2016 (UTC)

Classes\CLSID\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA} not found.

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}
    Class      => Groove GFS Browser Helper
    Module     => C:\PROGRA~1\MICROS~1\Office14\GROOVEEX.DLL
    LastWrite => Tue Dec 29 15:52:07 2015

Classes\CLSID\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43} not found.

{7DB2D5A0-7241-4E79-B68D-6309F01C5231}
    Class      => scriptproxy
    Module     => C:\Program Files\Common
Files\McAfee\SystemCore\ScriptSn.20160418115830.dll
                                                    Page 3

SOFTWARE OUTPUT.txt
 LastWrite => Mon Apr 18 15:58:30 2016

Classes\CLSID\{AE7CD045-E861-484f-8273-0445EE161910} not found.

{B4F3A835-0E21-4959-BA22-42B3008E02FF}
   Class      => Office Document Cache Handler
   Module     => C:\PROGRA~1\MICROS~1\Office14\URLREDIR.DLL
   LastWrite  => Tue Dec 29 15:52:07 2015

Classes\CLSID\{DBC80044-A445-435b-BC74-9C25C1C588A9} not found.

Classes\CLSID\{F4971EE7-DAA0-4053-9964-665D8EE6A077} not found.

----------------------------------------
bitbucket v.20080418
(Software) Get HKLM\..\BitBucket keys\values

Microsoft\Windows\CurrentVersion\Explorer\BitBucket not found.
----------------------------------------
clsid v.20130603
(Software) Get list of CLSID/registered classes

Classes\CLSID

Wed Apr 20 14:59:18 2016 Z
   {DFEAF541-F3E1-4c24-ACAC-99C30715084A}   Microsoft Silverlight
Wed Apr 20 14:56:11 2016 Z
   {B019E3BF-E7E5-453C-A2E4-D2C18CA0866F}   FlashBroker
   {D27CDB6E-AE6D-11cf-96B8-444553540000}   Shockwave Flash Object
   {D27CDB70-AE6D-11cf-96B8-444553540000}   Macromedia Flash Factory Object
Wed Apr 20 13:19:05 2016 Z
   {0D7C69CB-CF5F-4594-8FEE-0B6DDA9F75D6}   EpoEventInf Class
   {528F66A7-7891-4F6B-8F1E-5132CC80650C}   EventElement Class
Tue Apr 19 20:47:46 2016 Z
   {9D6AA569-9F30-41AD-885A-346685C74928}
   {D580254F-5E17-4AE0-9C41-60A0526A8ED6}
Tue Apr 19 20:47:45 2016 Z
   {F8BC3B89-DD15-4DA2-B936-CEA2B2A35053}   PSFactoryBuffer
Tue Apr 19 20:41:22 2016 Z
   {E6C0AE16-AE28-4c6a-884B-98F8B9AFBE6B}   MapiClient Class
Tue Apr 19 20:41:20 2016 Z
   {8885370D-B33E-44B7-875D-28E403CF9270}
Tue Apr 19 20:40:08 2016 Z
   {21CB022B-12DA-4981-97DF-6CDCA8615A05}   PSFactoryBuffer
   {61095308-52CE-433B-9A66-57B9E5835B60}
Tue Apr 19 20:00:03 2016 Z
   {71D96D48-D057-4CD1-AC31-E095EC268E0F}   CMSIWMIProvider Class
   {7ec522d9-de26-4f66-9a18-eb48144872af}   CPermissionWMIProvider Class
   {D463E764-205A-4B4E-AC79-EBC5A0EEB156}   CRemotePCConnectProvider Class
Tue Apr 19 20:00:02 2016 Z
   {01024B51-C524-42F7-8CCF-97AF361F8620}   CI Agent Startup Task
   {029A2C39-3654-43D7-935C-4B0B5F7C24C5}   Software Catalog Update Endpoint Startup
Task
   {02D2D25A-7E3F-4E23-89EB-1D876E9F6796}   Updates Deployment Automation Wrapper
   {070C8E43-8DD5-40A0-9E51-99571FCDD8AF}   DCM Agent Startup Task
   {0A4C6F71-CC04-4D2E-8949-F64A2EAB72F2}   MTC internal class
   {123E1CF5-298A-439B-AE46-10210FD420A3}   Power Management Manager Startup
   {12E72EDE-79C6-4CCC-8024-CD5CEE459072}   SMS SHA Shutdown Task
   {161808BB-22D7-4DC5-8051-1F50A635C707}   Service Shutdown Task
   {16589710-ACD8-4AAF-9658-B50DE773D45D}   Software Catalog Update Endpoint Logon
Task
   {173CB5AC-04E3-4380-BD63-DBBA69A933DC}   SMS AMT Provision Provider
   {1A09F592-1225-4D94-A587-54D52B859DD8}   VpnWMIProvider
                          Page 4

SOFTWARE OUTPUT.txt

```
{1AB3F060-0D2A-11DF-AB52-515456D89593}  CIObjectReferencePair Class
{1BE7281E-88F3-4ED2-BD4B-7CFEC9C2A06F}  SMS Specific Metadata used in SDM Models
{20E21465-8F14-4804-B9A3-8B03E7E86154}  AppExecutionLibrary
{21880E6D-CAF8-4D25-B96D-A39D1971D84C}  WebAppHandler
{218A1C12-46A7-4B6D-A629-EA812A53094A}  SMS SDM CI Factory
{257B8160-38BD-4F4E-8C16-6EC480B0E68A}  BITS2config
{26134FB1-2277-422F-902F-B5574DC8CFA9}  Service Startup Task
{29EE3E16-5DE1-48DF-B6EA-670B37D75504}  SMS Quarantine Configuration Compliance
Agent
{2D15EEE6-465B-40A1-B393-5D51B15FBE46}  Maintenance task coordinator
{2DB70103-3DFB-4806-85B0-B27B561284BB}  Updates Agent
{329E0625-C58F-4A93-B594-5A50ED00A4E0}  CI Downloader Class
{3B1826E5-6BFB-47A9-8370-0A6D8E61B74F}  DcmSQLQueryProvider
{3BBFB0B3-7AC8-4D45-852E-FBAB229C6E85}  AppVClientConfigCOM Class
{3FEBD542-4B9D-48DE-93B7-44B9E7337099}  ScriptHandler
{4180ACB0-4A34-11DE-BB09-568B56D89593}  IISProvider
{436EF0BB-F8D1-4635-BB22-6429D12CB90C}  VAppLaunchManager
{45B270B9-9A82-47E1-96E2-908535F3C365}  LegacyCmdLineScan Class
{4AF9B515-10F5-41AB-B0A6-B993957A73B0}  User logoff Task
{4D22ECDF-89E5-4E77-B034-9F6EEB997082}  ScanCompletionTask Class
{4D30CE7A-F6A2-408D-A5E9-394D8EA33155}  Power Management Event Monitoring Task
{555B0C3E-41BB-4B8A-A8AE-8A9BEE761BDF}  Configmgr Configuration Item WMI Provider
{5777363A-FB22-4A42-ABB0-522DD42711DC}  AppV Handler Class
{589D622F-C05D-48D8-977A-57ABF87655E8}  Updates Store
{59A392CA-B1C7-4F0E-89ED-64BD1A90ED87}  MTC PreStartup Task
{5B17A5D0-B569-4E49-90EE-00571C74013C}  UpdateStatus Class
{5B6CBE3C-CA4B-4207-89D9-45548AB42370}  Updates Deployment Agent Endpoint
{5B9C3324-906F-49EF-8318-41F9A07299A3}  AppV5XHandler Class
{5BAE1EF9-1CCF-413C-A0B2-0AB09543506E}  AppVMaintainer
{5F74328E-98B5-450A-8BB8-9DBDE6D887A9}  User logon Task
{6176C3DF-35A4-43F4-BBCE-96B497D27A61}  RegistryWMIProvider
{619524E2-A285-40F4-8BE5-1641AF150DE6}  Power Policy Handler
{62667615-5430-4559-AB26-B3A18BA29D0C}  BGB Client Agent Startup
{63608CB5-93D3-4953-A766-B817C8810981}  CI Tasks Manager Class
{699CD217-9C19-45B3-A93B-74EFE2FCE417}  User logoff Task
{6A5762D4-9023-498F-AD54-D1AC32064B0E}  CI Digest Store Class
{6DEF4741-BE43-42D3-84F4-31E0F9B4BEA1}  Applicability Broker Class
{76F76655-E0E4-4A4B-9BCB-B4B21A322E09}  DCM Agent Shutdown Task
{7AE81332-0D2D-11DF-AA79-ED7056D89593}  CCIRefObject Class
{80229306-C472-47A6-85FC-05479B278B30}  User logon Task
{811553DF-F796-4D15-98D3-9F2F0A4C654B}  ActiveDirectoryProvider
{81755C61-2323-47A7-BC08-FE0803B6A2DD}  OutOfBand Management
{837F7469-2D42-4982-A034-D8E71D2798CC}  SMS Update Instance Factory
{8593BF1E-B692-4ABA-98C5-3BA8150FBA3C}  User Session Reconnect Task
{86535867-52FB-408F-8419-414138196D63}  Power Management
{86CD77E3-85A4-408D-9C84-6D9B82CBA216}  App Mgmt SDK Interface Class
{870C8C55-0E15-4E2D-9D4B-76759315326C}  SMS Self-Test CI Handler Class
{884B90B6-6E0D-4B41-8B36-3D19137A6434}  CI State Store Pre OS Shutdown Task
{88CFBC1C-7424-4A0C-BA4D-9D3218143FD9}  CI Agent Shutdown Task
{8B1B4B43-7CDE-4113-BDF5-3A02EAEA9B16}  LocaAppHandler
{8F30D657-6D6C-45A5-9177-E35D1D55AAE8}  Power Management Manager Shutdown
{8F90B377-1DBE-434C-BAEE-B9E414185F3F}  CI State Store Shutdown Task
{8FDF5EC1-16A5-446B-92D7-29671B6C4B06}  Power Management Event Summarizing Task
{8FFA56F8-A1D4-4310-94FA-4BEB89D2A6E7}  SMS Power Policy Inventory Instance
Provider
{918989E1-A299-41C5-AD62-1F5F9336E11F}  Peer DP Manager Endpoint
{93EC4D65-A31F-4CD3-83D7-839243456FB3}  CCA Initialization Class
{941E1E62-7B5E-4371-9629-8EDDD1E2AF94}  FileSystemWMIProvider
{95106A3D-7DD3-42AA-9731-341C41B65FF8}  Bgb Agent
{95FF7127-4FE0-46B1-90FD-9ED4BBDE08EE}  VEProvider Class
{97FE2728-EBFB-4B2A-8CE1-4821191EF2B2}  Software Catalog Update Endpoint
{9E4429F1-2DBB-4CD0-9D4D-D01646DF81CB}  User logon Task
{9F3AA846-50B3-4CA7-8F0C-47FDC300B656}  CI Downloader Shutdown Task
```

Page 5

```
                        SOFTWARE  OUTPUT.txt
{A32E478C-C5E4-4C9A-9FF6-8978A14E9621}  Updates Store Automation
{A59E005F-A7B5-4E47-98E8-6A0B14320169}  CI State Store Class
{A85DCCE4-4CBF-4802-8066-D518A93DACAA}  UpdatesStore
{A91E8116-509D-11DE-BA23-CA9B55D89593}  UDAProvider
{AF4B0558-7BB6-455B-BD9B-B334342DF9B7}  CI Store PreOSShutdown Task
{AFE17F28-57B8-4A97-B21F-7F23A2C6FEAF}  ScanCallbackTask Class
{B07C1D3E-637B-4C71-BC2F-06665F376A59}  DCM Agent Class
{B20A2978-1F4D-11DE-94EC-334056D89593}  XMLProvider
{B298AF6C-1CBF-11DE-8BC8-522756D89593}  DcmWQLProvider
{B6F3B912-A3C6-466D-8EE0-C09B0F63563F}  Updates Deployment
{B7D64AEC-7459-4121-8884-CA8BA4CC99B0}  CI Store Class
{B90044A8-93E5-4ACF-916E-67C03181206B}  BGB Client Agent Shutdown
{B933785F-9D22-4D3B-A469-B8C180C447C7}  MsiHandler
{B9C9F542-AC54-11DD-B237-0EBC55D89593}  SUMProvider
{BAFBA325-0E26-4719-990E-C3A18D3B5B6B}  Service Shutdown Task
{BDBCE7D6-E729-427E-8F19-78E72251C453}  NotifyContentProgress Class
{BFD31CA1-0800-40B5-9A34-DE3BDDCD6BDD}  ScriptProvider
{C2ADB1BC-7FCC-41B0-BE48-B0950048990F}  WMIDiscoverySource
{CB29C718-CB3D-449B-9242-5C92E9941A60}  DCM Reporting Class
{D080BE9A-5A90-463A-B701-1CD0B71AF699}  AppProvider
{D5BE5151-C449-4318-859B-69023A1B396E}  Targeted Updates Manager
{DC3EF378-2ABA-45A2-A773-4BCC61938F59}  CI State Store Startup Task
{DD20FF75-3D54-477C-AF5E-AFEC5D89BF25}  Update Discovery Provider
{DD836951-2E44-489A-946D-F232F659E521}  TS Agent
{DE2955A7-63CF-48BA-AC82-6E8961B03A48}  WUAHandler
{E0DF4BAD-303C-4023-BFB8-4C8217CD9720}  CI Downloader Startup Task
{E17D9FF9-AF9F-4EE2-A35C-5B092C7DDF30}  Scan Agent Endpoint
{E24F0E9A-E227-411E-9732-8778AFB48B09}  ScanTool Class
{E2F95B1F-1A1D-468B-830C-62794CAF0943}  DCM SDK Interface Class
{E40745A1-F35A-48B1-A05D-29E6947C5C85}  UpdatesScan Class
{E4A3AB31-19A6-442C-A8CF-C1F69B929B62}  AppLaunchStateManager
{E53041E3-7C0B-491B-B638-CAB8078F57F4}  ExpressionSolver
{EB129C7B-918F-4D01-873F-4E89685F044F}  BGB Action Message Handler
{ECC8995E-4C99-11DE-81CF-03D255D89593}  AssemblyProvider
{ED3FD5C2-1ECD-4D89-A994-9F2F31FBF9A3}  'CI Store Shutdown Task
{EE0D6DEE-2DEB-4553-9E60-26D911EF081F}  SMS AMT Inventory Instance Provider
{EE1BD859-AACD-48FE-A9B6-9358DC21ADAE}  ConfigMgr SHA Info
{EE8CC9D5-6896-4F98-83F7-601DFB67BCAA}  AppVManageCOM Class
{F3D6370B-6E1D-4A6D-AF6A-66D2ADB2B01C}  CI Store Startup Task
{FB7A65D7-3060-4AEB-93CD-8311D4FD4F46}  GlobalExpressionValueProvider
{FE6F65AD-F204-4485-813E-818BD1803413}  ScanAgentStartupTask Class
{FE98DDE9-E725-4492-BAD6-0E9B0C47744F}  CI Agent Class
{FEC637BC-8AEA-4CA4-9F90-948616C02A86}  Power WakeUp Task
{FF44331F-A337-470C-99B5-EAEAED6A953F}  AppVPackageQueryCOM Class
Tue Apr 19 20:00:01 2016 Z
{0362A876-DEED-41E2-9C43-88E5AE953288}  MIF group instance provider
{045A0AA9-A9B2-4156-B8D3-25D5A6F49510}  Status Agent Shutdown Task
{0536C386-CF4A-4785-8854-E316081986CF}  Client Inventory Data Store
{05D1D5D8-18D1-4B83-85ED-A0F99D53C885}  CCM WMI Event Provider
{0797FA65-B140-4AD8-BC24-7E702C855337}  Content Transfer Manager Startup Task
{07F81A45-04E4-4605-A945-A0DB3F720544}  Software Center Endpoint
{089CB9E7-99E4-4973-BA3B-F63C7C26A8C9}  Client Components
{096C5BA8-044B-4BAC-9914-144723BA4F2A}  CP Applet Manager
{0AF18720-092F-44DE-A46E-8473C3CEBAE1}  Policy agent post startup task
{0BA08E88-A9EB-4058-AA72-A9EB8DD5B2F4}  CCM Policy Agent
{0D011B6A-4BDB-49CB-8533-820B75E24DCA}  CCM Service Administration Class
{0EB9E5B3-21C8-4724-BF74-388164088C95}  Location Services Maintenance Task
{0F95BCE5-2209-488A-B4BC-4396AD233C8D}  SMS Client Service Error Handler
{111F6CCB-0304-4081-91E0-61846BEE57C3}  CTM Data Transfer Service Reply Endpoint
{135D7881-D666-4046-A1DF-7EC7B5785A67}  Content Cache Manager
{150DEE35-FD08-4684-96E2-619399CFBF94}  CCM HTTP Post class
{167B611B-D321-46DA-B344-43FAF5296940}  CCM Policy WMI-XML Action Handler
{16D14FC2-CF84-4DA8-8896-9B573F10BFAB}  State Message Provider
```

Page 6

```
                          SOFTWARE  OUTPUT.txt
     {17E58800-8549-444B-B1E2-5DB454B4DBE8}  CCM Policy Agent ReRequest Policy Endpoint
     {18B4D28B-B5ED-4FA9-9F0B-449F6A3906DF}  CCM Client Identification Manager Startup
Class
     {18E89A5A-D91F-4BAF-9272-289767F5212A}  Client Properties
     {19365BEF-50B9-4C54-8625-770EE1A5D8B0}  LS NAP Initialization Class
     {1CCB96F4-B8AD-4B43-9688-B273F58E0910}  CCM ISensLogon2 Implementation Class
     {20C15473-0F6D-4877-A13A-EB9DCFF4F843}  User Logoff Task
     {2346FA0E-633F-411A-991D-EEF7612D5045}  SWDistClientSettings Class
     {2410CAC5-AB48-4AB8-8725-9BF0625C2B94}  Sms Client WMI Method Provider
     {25AF1DB8-69AE-42F4-8DE3-123BC07BD7E4}  ClientAgentSettings Class
     {26C5C734-740F-4060-99E1-65DED20A275D}  Client Remote Tools Configuration
     {27F6C721-3343-4583-AA3F-A9B7B5BBA16F}  Hosted Software Center Manager
     {2A552830-5C99-4D45-91B4-8AD37D3B1B96}  Client Evaluator Startup Task
     {2AE987B9-18A2-4961-A91C-197FBE103535}  Source List for Windows Installer Product
     {2DA346D3-3D88-4393-A8F8-7B7410657F21}  CCM Client Authentication Hook
     {2E48AA12-2801-11D3-88DA-00105A1F82ED}  SMS Logical Disk Instance Provider
     {2F382DC1-FF25-486E-896F-60AB49ABB410}  CCL Location Services Reply Locations
Endpoint
     {2F768BE3-61D1-4946-A98D-25A6AA2E3C25}  SuperPeerController Agent
     {30FE11D5-5FA6-42CF-AB38-9128202E8864}  Status Agent Startup Task
     {3496431A-7EF8-4FB7-AEDE-C875267740E0}  CacheElement Class
     {3867E993-E1EC-11D2-846E-00105A1F7D6D}  SMS Instance Provider
     {3BDC8FB8-F1ED-4A6E-963B-EFA9FF24E711}  CTM Location Service Callback
     {3E8CA3C9-E00E-48E9-B249-CA6C65E4A69A}  CacheElements Class
     {3EBECAFE-6A49-40FF-B51E-6A6E0933A636}  SMS Client Event Forwarder
     {41CDA4B1-43F5-4044-B44F-A548E62A4C5A}  Service Startup Task
     {4221FFD7-AEFA-48CF-A33C-06E39F796A67}  CCM Scheduler Logoff Class
     {42992500-03F8-4E2E-919C-D9BE3DB72E50}  State Message
     {4310C4C4-0F7E-46E3-B05E-F0D4FB382D71}  CCM XML Store Manager
     {432848E6-20A1-4CC7-AFA6-7A3416881593}  SmsEventLogForwarder Class
     {437E822C-8337-4E70-A03B-B75E79D7B975}  Software Metering Manager Shutdown
     {451F8ED4-D182-4CF6-8251-337EC7FF577D}  Source Update Manager Endpoint
     {492FB744-29DD-4EE6-98E3-D14DCF3CF390}  Ccm Proxy Manager
     {49507317-AA1F-4FB2-B9EF-52BCF10D5A71}  DDR Instance Provider
     {498C5E85-FFF2-4B1C-B635-1953CCD9ED5E}  CCM SID Client Identifier
     {4A77680E-BC69-466D-BFF3-D9E01E9B633D}  CheckContentAvailability
     {4BDA5DF8-9A53-4761-86CA-A0C95E3B1426}  Content Access Service
     {4DA93899-0B99-43E1-AB88-D80DFC232A55}  CCM HTTP message class
     {4E9DCC5B-A1BF-436C-9AC0-5CE1E022ED31}  CCM Policy Agent Policy Evaluator Endpoint
     {50DC39EC-30A2-4FEC-87CA-E54F67944474}  CCM Policy WQL Expression Handler
     {5179B48C-C9FB-4CE1-B0EA-C3BF0E68C04C}  Software Execution Ex
     {52C72C90-A4C4-4263-B771-055524FA2507}  FileBITS Logoff Task
     {53E037F3-7ED6-4AB3-9C4B-33AC188CF130}  Software Metering Manager (Serial)
     {53FC6137-F53B-4411-BCEB-7810CC712344}  Client Property
     {563803BF-C2B6-4993-A059-8E3DBE7E314D}  UI Event Class 2
     {56402E94-1109-452D-BFE9-B2CCC0F8D83E}  CCM SMBIOS Client Identifier
     {57985DF7-569A-484A-A2E6-70F100024340}  Data Transfer Service Startup Task
     {57C0AFD2-2895-4304-9DDB-1445A9A7BBC6}  Client Remote Tools Policy Configuration
     {58E2FE09-07BB-4ADB-8A93-E49C5BF2301F}  Client Inventory File System Query Task
     {5A97C631-CA21-4595-B1B8-EB6C47D34051}  CCM Policy Agent Policy Download Endpoint
     {5BECBDD8-9DD9-435E-88AA-4C62BBDA74AD}  Content Transfer Manager
     {5C3A4CA0-BE8A-46DE-BFF2-AA552C4CED79}  Software Center Logoff Task
     {61CC81F8-8F91-4E96-B707-BA45D2330DCB}  Client Inventory Collection Task
     {6297829C-7476-4255-9239-37F5FB1DD868}  Client Inventory WMI Utilities
     {64E0F19B-5014-4AD7-BE78-7F0D8297EC90}  System Device Instance Provider
     {66508F24-5509-422D-B98D-C517A19CC03D}  FileBITS Logon Task
     {66BBFD4C-BA77-466C-ACEB-A1808564A17A}  ProcessEventProvider
     {69794D1B-E3D0-4D08-A9CA-0B54FE1C1776}  SHA Endpoint
     {69D999DC-0648-420F-9787-36F381067BD6}  Client Action
     {6B6662B9-CA7B-4A08-82D9-C0BC1291B260}  Service Startup Task
     {6B84FE09-4914-4CF9-A32F-71E7B7C3391E}  User Logon Task
     {6BBDFEDC-261A-4EA8-B23A-1357700E441B}  SMS Framework Event Forwarder
     {6C73E502-86FF-49B6-B44A-A641CF46E36B}  CCMSDK Provider
```

Page 7

```
                       SOFTWARE OUTPUT.txt
{6FB530C5-6EED-4AB1-9654-420A80E52C21}  CCM Content Location Services
{70C6CDDA-E74F-48F3-9F12-2FC9192E778F}  SMS Policy Event Forwarder
{72451213-A98F-4769-BB5C-E425117470AA}  Program properties
{73DE0F4D-7E4D-42E2-8080-3EAD934B88E8}  CCM Message Authentication Hook
{748FFF62-0721-4BAB-9C22-F0A25C2C42B2}  CCM Policy SDK
{74C50AEB-19A8-4218-9A9E-02C208488136}  Network Changed Task
{750D84E5-20F6-47B7-A5E3-66C16B193049}  CCM Location Services Scheduled Cleanup
{7B9F3246-A56A-489F-8B41-CBA984C17194}  CCM VDI Property Mapping Provider
{7BB3BE07-96FC-40A6-89CD-E2180149A266}  Remote Tools Agent Endpoint
{7DBDD3CA-11BD-406C-9EE4-B0AAE170EE2E}  UI Resource Manager
{7E89FF0B-F649-4F9A-A9C3-F05DFAAA3DA1}  CCM ISensLogon Implementation Class
{7EE84FE5-0A01-4211-BAE1-CA04E956E13B}  Software Center Shutdown Task
{7F1A2A2C-2167-47A1-BCB7-973D05C0CF5F}  CCM Scheduler Startup Class
{80A05E30-1FBD-4883-A230-058D8F6CED74}  Power state manager system task
{84ECA343-5158-48BB-87C3-37EF4B919F20}  State Message Manager Endpoint
{858AA283-870F-49A5-ACE1-1C6CD20822B0}  Service Shutdown Task
{86875FDD-EB5D-4742-8026-94B2E31E1AB9}  Asset Advisor WMI Instance Provider
{884E3B2A-265B-4E7B-9C10-23E1DA25238A}  User Logon Task
{89EFC930-2657-449B-A39E-DB9CDD311C4F}  Software Center Manager
{8A579C35-8D13-4559-89E1-8F4039C18DFF}  Ccm Network Proxy Services (Ex)
{8C3F84DE-9596-4C99-B5A8-BE31178C2338}  CCM Policy Agent Request Assignments
Endpoint
{8C8E04F0-5C74-4461-8AFF-EE3F8C39F3B6}  ServiceWindowManager Timer Task
{8EC7E83E-3F67-414B-A9EC-86F0E36DC619}  CCM Registration Endpoint
{8FB276D1-972A-4DDB-AD8C-5377FCE79653}  ServiceWindow Handler
{915EC5BC-89A3-495E-8E99-C2DD8049DFD8}  Client Actions
{917A8909-DC5B-4A37-9386-B2CDAC8E66F2}  Service Startup Task
{924C2EDC-6A37-4DB5-8461-E88961E19B27}  Software Center Startup Task
{92652E89-6F26-4649-A319-E8E0F4858BB8}  CCM Authentication Hook Maintenance Task
{947B1B47-38BD-4F59-862F-C504ED30E5DA}  User Affinity Provider
{949EB962-1542-40F2-A703-348BF490CEF0}  Asset Advisor Component
{95F0BCE4-F21B-11E1-AA55-1D456288709B}  Password Settings Provider
{966FEDB0-2E21-4E5B-848D-797AA90DA80E}  Configuration Manager System Health Agent
{98651EBC-3820-4BC2-BA89-189A5C6C7EBC}  CCM Message Encryption Hook
{994A7A85-B75B-4F34-8B34-842FD70C830A}  Software Metering Manager Startup
{9967A433-A640-4A56-8C3D-D8E8F95FF8F3}  Sms Client Manager
{9A072C42-7860-4B6A-82B7-623AEE7C7436}  State Message Eventing Class
{9EF8EBF8-93CD-4139-8C99-61F27FE2859A}  CCL Location Services Network Config
Endpoint
{A07AAC0B-D31A-4F53-9857-BE2B42D80B49}  CCM Scheduler Logon Class
{A0907896-081C-4A2B-B4BC-18E42BFE5100}  Source List for Windows Installer Product
{A21EF016-C5FB-4040-A07D-F254B5B63453}  Client Registration Startup Task
{A2237358-F094-43AF-B0AD-75EC2E3DCDCB}  Location Services command handler
{A3657EA6-6E04-479D-AB40-6185533EB79D}  Service Shutdown Task
{A3A4B535-C526-42B2-9236-90D460F9FEF7}  CCM Scheduler Shutdown Class
{A3B5BAB0-17B2-48F5-B5E2-FB8727D93A6F}  Maintenance Mode Manager
{A8889E84-14D9-43D0-813A-249BFFE193C2}  CCM Scheduler Schedule Info Class
{A8E82667-5C4F-41C0-8056-E856D2B04C44}  User Affinity Logoff Task
{AA7F0969-09E2-4D7E-8E61-BFFC3A7FF689}  CCM Policy Agent Reply Assignments
Endpoint
{AB008B5A-29B3-4DE0-9930-A9004F8C9F3F}  CCM Certificate Maintenance Endpoint
{ABA57BB9-5DFA-49FE-9A60-B494BF883F19}  CCM Profiler System Task Class
{AD1E7DD3-4701-4A54-9385-D61F58FA4E14}  Execution Engine
{AE184660-8F00-4C31-95BA-33A060E0C9CC}  Client Inventory Agent State
{AE483254-AAF0-4083-AA18-32C5479E6DCC}  CacheInfo Class
{B019CAE0-D910-410F-AD15-5AFA0E58DF61}  Messaging Service
{B2FF5EE8-CCD0-43E3-BB44-BD7D7E206040}  UI Event Class 3
{B61B02C8-6F75-4F74-9FA4-EEA5F391A425}  Data Transfer Service
{B837493E-0508-4086-AD41-DC642915B3DD}  Messaging Request Response Handler
{B83AEF0D-BE20-45A4-8932-5787371FCE6B}  Client Inventory Report Task
{B9C6E505-98B8-4CDC-97DE-C6787C420EF6}  RDV Identity Store
{BA9313BF-AF06-4F18-949E-82A861AF2D57}  CCM Policy Agent WMI Replication Event
Consumer
```

Page 8

```
                    SOFTWARE OUTPUT.txt
{BB3BBF79-FBD8-46F0-B9C3-AB1A69EB3015}  CCM HWID Client Identifier
{BB870E66-9DB8-49D1-921E-14C87570124C}  Client Registration Timeout Task
{BE55EEAE-EFBC-45A8-9D9C-0F34C8824B1A}  CCM Command Invoker Class
{BF6D8B7D-D672-4221-84F4-16657A654909}  Execution Status
{C0ED66AD-8194-49FD-9826-D0DD38AB7DAA}  Client Inventory File System Collection
Task
{C36F6DB3-F7A5-40FE-94B2-E1C2D4DE20B2}  User Logon Task
{C50E9002-F397-4402-BF78-07194C5DA599}  Service Startup Task
{C58C6E9C-2C1D-4823-B1F8-B0966A3DACD2}  UI Event Class
{C612F052-C85C-4156-B974-87947FAA7569}  SMS ARP Publisher
{C655AFCA-70CB-4C27-8FB3-3D2A90529C34}  Data Transfer Service Logon Task
{C7A1C224-50F7-4961-AFBA-C7BEF8FFDD60}  CCM Location Cache
{CA227B79-697F-4ECE-9D4E-A0C6B42C7832}  Software Metering Report Generator
{CBE27977-BB1D-4984-9BF8-DE8B19EF9601}  SMS ZLib Compression Hook
{CE22C5BA-165D-4B93-BC73-926CE1BD9279}  Client Inventory File Collection Task
{CEDEE1F0-8763-4D41-8C38-449F58C24D25}  SMS SHA Binding
{D6C2C3A7-BE03-457D-9A79-CEF973B221A5}  Service Shutdown Task
{D6E8E829-A355-4706-A7DA-2AB8E323DAB7}  Location Services Network Changed Task
{D8AB0A9B-DCE9-4F92-87CB-67E72862B2C0}  Software Center Logon Task
{D94768A8-18CA-4018-8ECA-6A22F0A4E6C9}  Service Startup Task
{DF75308D-0DF4-428B-952C-EBFF36DBA3CB}  Reboot Request
{E0968C45-7DE0-4ED8-8ADC-550BD20161BB}  Client Inventory Agent Endpoint
{E0C5ED5F-8582-4444-AF7D-52A3FEAA6A35}  Embedded Inventory Provider
{E2B4C3C6-BB91-47D1-B564-5C6A0FBB1CE4}  ServiceWindow Manager
{E333E5E5-368A-402B-8E80-14E292554B33}  Program collection
{E73CB269-A663-43D2-A05F-8020B9CCC37E}  Affinity Agent Startup Task
{E90F8BCE-FB4B-485D-B84B-8010283888C5}  Client Component
{E94C4865-9BD2-4314-8A9D-6DBDD0333085}  FileBITS Startup Task
{ECE79E71-2AC6-4A26-8D20-7A1E0A4D7A6D}  Reboot Coordinator
{ED7C8B62-BB7C-498E-B858-298B5E697817}  CCM HTTP Class
{EECA3D86-F60F-4646-8D47-07A371EE4BF5}  Execution Manager Endpoint
{EEF81F9C-8E96-43FA-89A3-0D9686CEB518}  User Logoff Task
{EF9B9B0B-009A-41F5-AF21-6AD433868C4F}  Inventory Provider
{F13946FA-8641-4B12-8BC0-2868D45D62FF}  Policy evaluator system task
{F3133CB2-03F7-4145-9DA5-C437898163C9}  Status Agent Standard Event Forwarder
{F3C6E2A5-44B9-47B5-B2BD-97A29262D9EF}  User Affinity Logon Task
{F59630CC-3FE3-4306-9BD1-1E4270333F12}  CCM Policy Agent Cleanup Endpoint
{F5C3DE16-1EFC-471F-B94D-A8D18319DE30}  SMS Event
{F5D0AC1B-4B63-4187-9F48-A3B759CD791E}  CCM WSUS Location Services
{F7B8AAB7-0C97-44A6-8308-36E9EDF95ABA}  Timer Task
{F80A8D57-D338-43FF-A5E6-5D093EA80775}  CCM Client Action
{F940F973-3D7D-4344-BCDC-942A8698F2B1}  CCM NAP Location Handler
{FBA8EA8E-B80E-4B46-BD44-1AB03F99E8BB}  CCM Policy WMI-MOF Action Handler
{FBCE4709-6098-43C6-9211-BBDCC188B591}  CCM Policy Agent WMI Instance Provider
Tue Apr 19 20:00:00 2016 Z
{1EF9F1AB-8047-4952-8AC4-B6C7CCE87AF9}  EP Agent Startup Task
{2B0704D2-E90B-4491-9595-CCFBBF9BBC41}  SMS EP agent
{2C1E6553-80F4-4EFD-88A5-B5090BEF2615}  CCM Debug Log
{465D6FE5-3FC1-4B3E-9787-22E9E1BD3402}  SMS Exrternal Event Agent
{8290DEB8-2E2B-48B2-B38E-5AD9A90DF285}  External Event Agent Startup Task
{CD506EC4-7C8A-4D28-93B8-C872A9E73F6E}  SMS Compression Hook
Mon Apr 18 16:25:28 2016 Z
{7160A13D-73DA-4CEA-95B9-37356478588A}  CUIExternal Class
Mon Apr 18 15:58:31 2016 Z
{6D51AC3F-7048-4C0F-9831-18E4F701EF86}  MfeAddin Class
Mon Apr 18 15:58:30 2016 Z
{7DB2D5A0-7241-4E79-B68D-6309F01C5231}  scriptproxy
Mon Apr 18 15:58:26 2016 Z
{cda2863e-2497-4c49-9b89-06840e070a87}
Mon Apr 18 15:57:48 2016 Z
{3627944C-4353-4d18-BF54-B4AB59637818}  Pointsecprovider
Mon Apr 18 15:56:59 2016 Z
{988248f3-a1ad-49bf-9170-676cbbc36ba3}  DNE Filter Configuration Notify Object
                         Page 9
```

SOFTWARE OUTPUT.txt

Mon Apr 18 15:56:54 2016 Z
```
  {C15C0AAF-C309-FE12-BB17-814630A2009F}  Cisco AnyConnect Secure Mobility Client
Pre-Logon Access Provider
```
Mon Apr 18 15:54:54 2016 Z
```
  {0A4C50AC-AD3F-4245-B324-3C8696A3408A}  WbxAction Class
  {4D185FEC-958C-4DB4-87AA-D4D79A46FAB7}  WebExRightMenu Class
  {80947ADC-151D-490B-87F1-7C8CE1B46220}  WebEx Productivity Tools
  {90E2BA2E-DD1B-4cde-9134-7A8B86D33CA7}  WebEx Productivity Tools
  {AEECE333-8900-4915-9697-7A0B4034B3D8}  WebExWordAddIn Class
  {C3741FD4-FABE-4C36-88E7-40C0C09FCE8D}  WbxPPTAddIn Class
  {C5702709-844C-4A86-9C05-F2D3E58FA6D5}  PSFactoryBuffer
  {E8D0CE8D-BC70-4025-978F-E86068362730}  UserNameHolder Class
  {F6E0DEDD-F6D5-4195-BE2D-AB628A0BBDF4}  WebExExcelAddIn Class
```
Mon Apr 18 15:54:53 2016 Z
```
  {4DEB3D89-D0D0-47CB-8DE7-9080B8F3B143}  CiscoPTOutlookAddin Class
  {7F9135D2-9B91-43A1-B0AD-5EC39BB69209}  CWaiterApp Class
  {BAEE998A-9C95-4966-8E52-DBCA67D8482A}  PaneContainer Class
  {EA47D2DE-76CC-4138-97FF-A62F9D28A341}  Addin Class
```
Mon Apr 18 15:51:11 2016 Z
```
  {0002DF01-0000-0000-C000-000000000046}  Internet Explorer(Ver 1.0)
  {00C429C0-0BA9-11d2-A484-00C04F8EFB69}  CrBlinds
  {0358b920-0ac7-461f-98f4-58e32cd89148}  Wininet Cache task object
  {049F2CE6-D996-4721-897A-DB15CE9EB73D}  Iris
  {057EEE47-2572-4AA1-88D7-60CE2149E33C}  PSFactoryBuffer
  {05BDC38E-5493-487a-A7FF-8CF2246ABC13}  IE Background Task Scheduler
  {05f6fe1a-ecef-11d0-aae7-00c04fc9b304}  IntDitherer Class
  {06EEE834-461C-42c2-8DCF-1502B527B1F9}  URL Shortcut PropSetStorage Mapping
  {07C45BB1-4A8C-4642-A1F5-237E7215FF66}  IE Microsoft BrowserBand
  {08165EA0-E946-11CF-9C87-00AA005127ED}  WebCheckWebCrawler
  {0968e258-16c7-4dba-aa86-462dd61e31a3}  PersistentZoneIdentifier
  {098870b6-39ea-480b-b8b5-dd0167c4db59}  IE OpenService Manager
  {0b6d74fe-ad29-4c92-ac06-f06bc2f238a7}  Microsoft Feeds Request
  {0C7EFBDE-0303-4c6f-A4F7-31FA2BE5E397}  AlphaImageLoader
  {0E890F83-5F79-11D1-9043-00C04FD9189D}  DXSurface
  {10BCEB99-FAAC-4080-B2FA-D07CD671EEF2}  IE Recovery Store
  {11016101-E366-4D22-BC06-4ADA335C892B}  IE History and Feeds Shell Data Source for
Windows Search
  {164484A9-35D9-4FB7-9FAB-48273B96AA1D}  RadialWipe
  {16B280C5-EE70-11D1-9066-00C04FD9189D}  Fade
  {16B280C8-EE70-11D1-9066-00C04FD9189D}  BasicImage
  {16d51579-a30b-4c8b-a276-0ff4dc41e755}  JScript Language
  {181D6C15-60A6-4BC7-A8E7-389D5BFE4841}  Reading Mode Viewer
  {182C3813-DF97-40fa-9C4E-B7D3E74F00CA}  Pinned Site Shortcut
  {18845040-0fa5-11d1-ba19-00c04fd912d0}  Microsoft HTML Load Options
  {19916E01-B44E-4e31-94A4-4696DF46157B}  InformationCardSigninHelper Class
  {1a6fe369-f28c-4ad9-a3e6-2bcb50807cf1}  Developer Tools
  {1C1EDB47-CE22-4bbb-B608-77B48F83C823}  IE Fade Task
  {1D1F0730-0748-4b5f-81DF-865694BD07AC}  IE OrderListExport
  {1E54333B-2A00-11d1-8198-0000F87557DB}  DXLUTBuilder
  {205D7A97-F16D-4691-86EF-F3075DCCA57D}  IE Menu Desk Bar
  {20CCEF1E-0185-41a5-A933-509C43B54F98}  ShdocvwBroker
  {2183DACA-D0BF-4a31-97F7-B87618A81955}  IE Shared Task Scheduler
  {23E26328-3928-40F2-95E5-93CAD69016EB}  ZigZag
  {25336920-03F9-11CF-8FD0-00AA00686F13}  HTML Document
  {25336921-03F9-11CF-8FD0-00AA00686F13}  Microsoft HTML Document 6.0
  {28BCCB9A-E66B-463C-82A4-09F320DE94D7}  F12 Developer Tools
  {2B4F54B1-3D6D-11d0-8258-00C04FD5AE38}  Shell BindStatusCallback Proxy
  {2BC0EF29-E6BA-11d1-81DD-0000F87557DB}  Convolution
  {2E7700B7-27C4-437F-9FBF-1E8BE2817566}  RandomBars
  {3028902F-6374-48b2-8DC6-9725E775B926}  IE AutoComplete
  {3050F391-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML Window Security Proxy
  {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML Javascript Pluggable
Protocol
```

Page 10

SOFTWARE OUTPUT.txt

```
{3050f3B3-98b5-11cf-bb82-00aa00bdce0b}   %Microsoft Image Element Browse Property
Page%
{3050f3B4-98b5-11cf-bb82-00aa00bdce0b}   %Microsoft Document Browse Property Page%
{3050f3BB-98b5-11cf-bb82-00aa00bdce0b}   %Microsoft Anchor Element Browse Property
Page%
{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTML Resource Pluggable Protocol
{3050F3C2-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTML DwnBindInfo
{3050F3D6-98B5-11CF-BB82-00AA00BDCE0B}   IImgCtx
{3050F3D9-98B5-11CF-BB82-00AA00BDCE0B}   MHTML Document
{3050f3DA-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTML Mailto Pluggable Protocol
{3050F406-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTML About Pluggable Protocol
{3050f499-98b5-11cf-bb82-00aa00bdce0b}   Microsoft HTML Recalc
{3050F4CF-98B5-11CF-BB82-00AA00BDCE0B}   PeerFactory Class
{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B}   HTML Application
{3050f4e1-98b5-11cf-bb82-00aa00bdce0b}   HtmlDlgHelper Class
{3050f4f5-98B5-11CF-BB82-00AA00BDCE0B}   Trident HTMLEditor
{3050f4f8-98b5-11cf-bb82-00aa00bdce0b}   Microsoft Html Component
{3050f5be-98b5-11cf-bb82-00aa00bdce0b}   DownloadBehavior Class
{3050F5C8-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTA Document 6.0
{3050f664-98b5-11cf-bb82-00aa00bdce0b}   LayoutRect Class
{3050f667-98b5-11cf-bb82-00aa00bdce0b}   Microsoft Html Popup Window
{3050f67D-98b5-11cf-bb82-00aa00bdce0b}   Microsoft Html Document for Popup Window
{3050f6b3-98b5-11cf-bb82-00aa00bdce0b}   Template Printer class
{3050f6cd-98b5-11cf-bb82-00aa00bdce0b}   HeaderFooter class
{3050f6d4-98b5-11cf-bb82-00aa00bdce0b}   DeviceRect Class
{3050f819-98b5-11cf-bb82-00aa00bdce0b}   HtmlDlgSafeHelper Class
{30510483-98B5-11CF-BB82-00AA00BDCE0B}   Microsoft HTML Element Context Stream
{30590066-98b5-11cf-bb82-00aa00bdce0b}   SVG Document
{30590067-98b5-11cf-bb82-00aa00bdce0b}   XHTML Document
{30C3B080-30FB-11d0-B724-00AA006C1A01}   CoMapMIMEToCLSID Class
{32374F0E-85D3-4408-9BD0-887E3EEAE7F0}   IE JScript Profiler Core
{32B533BB-EDAE-11d0-BD5A-00AA00B92AF1}   AP Class Install Handler filter
{333C7BC4-460F-11D0-BC04-0080C7055A83}   Tabular Data Control
{34a13fc7-86ab-42e6-a32c-b50666f04ff9}   JScript Language Authoring
{34a3d570-67d9-4265-a9ee-8c3fa3dfeccf}   TravelLog
{34e6abfe-e9f4-4ddf-895a-7350e198f26e}   Microsoft Feeds Arbiter LoRi Broker
{374CEDE0-873A-4C4F-BC86-BCC8CF5116A3}   IE HomePageSetting
{385A91BC-1E8A-4e4a-A7A6-F4FC1E6CA1BD}   DXTFilter
{3A04D93B-1EDD-4f3f-A375-A03EC19572C4}   MaskFilter
{3BC4EE9F-1FC1-44DB-81FA-AD94DEC7AF30}   CLSID_AppRep
{3C374A40-BAE4-11CF-BF7D-00AA006946EE}   Microsoft Url History Service
{3CB169B3-17D9-4E47-8B93-2878998F69A2}   WebBrowserHandler Proxy
{3DC7A020-0ACD-11CF-A9BB-00AA004AE837}   The Internet
{3dd53d40-7b8b-11D0-b013-00aa0059ce02}   CDL: Asychronous Pluggable Protocol
Handler
{3E669F1D-9C23-11d1-9053-00C04FD9189D}   DXSurface Modifier
{3e71f26d-136f-4545-813f-35276024b705}   XML Feed Subscribe Dialog
{3F4DACA4-160D-11D2-A8E9-00104B365C9F}   VBScript Regular Expression
{3F69F351-0379-11D2-A484-00C04F8EFB69}   CrIris
{421516C1-3CF8-11D2-952A-00C04FA34F05}   Chroma
{424B71AF-0695-11D2-A484-00C04F8EFB69}   CrRadialWipe
{429AF92C-A51F-11d2-861E-00C04FA35C89}   %Trident API%
{4356b08e-ecb5-43d1-8e9f-7bef4fc960fe}   Manage Add-ons Admin Broker
{43886CD5-6529-41c4-A707-7B3C92C05E68}   IE Navigation Bar
{43A8F463-4222-11d2-B641-006097DF5BD4}   Shell Name Space ListView
{447EDBE5-0080-4036-A0BB-7B84C58C604F}   IEDataObjectWrapper
{44C76ECD-F7FA-411c-9929-1B77BA77F524}   IE Menu Site
{46CB32FA-B5CA-8A3A-62CA-A7023C0496C5}   CIEContentAdvisorBroker
{473AA80B-4577-11D1-81A8-0000F87557DB}   DX2D Anti-Aliasing
{4A03DCB9-6E17-4A39-8845-4EE7DC5331A5}   Spiral
{4ABF5A06-5568-4834-BEE3-327A6D95A685}   Matrix
{4b360c3c-d284-4384-abcc-ef133e1445da}   CIERegistryHKLMBroker
{4B78D326-D922-44f9-AF2A-07805C2A3560}   IE Menu Band
```

Page 11

SOFTWARE OUTPUT.txt

```
{4C6470A6-3F91-4f41-850B-DB9BCD074537}  Microsoft Feeds Background Sync Component
{4CB26C03-FF93-11d0-817E-0000F87557DB}  DXTaskManager
{4CCEA634-FBE0-11d1-906A-00C04FD9189D}  Pixelate
{4D5C8C2A-D075-11d0-B416-00C04FB90376}  Microsoft CommBand
{4DFED3F9-B794-4d3c-973B-DDA1C28105A9}  Private Profile Object
{5220cb21-c88d-11cf-b347-00aa00a28331}  Microsoft Licensed Class Manager 1.0
{528d46b3-3a4b-4b13-bf74-d9cbd7306e07}  XML Feed Document
{53510d24-57eb-4713-9afb-e6e60530b87e}  IE RSS Feeds Tasks
{54702535-2606-11D1-999C-0000F8756A10}  Text Label Class
{55136805-B2DE-11D1-B9F2-00A0C98BC547}  Shell Name Space
{553858A7-4922-4e7e-B1C1-97140C1C16EF}  IE Component Categories cache daemon
{555278E2-05DB-11D1-883A-3C8B00C10000}  Scale
{55b70dec-4b3b-4e26-ae9c-9e8d131843a1}  Microsoft Feeds Background Task Scheduling
{5AE1DAE0-1461-11d2-A484-00C04F8EFB69}  Wheel
{5bbd58bb-993e-4c17-8af6-3af8e908fca8}  IE Spelling Dictionary Installer Broker
{6038EF75-ABFC-4e59-AB6F-12D397F6568D}  IE Microsoft History AutoComplete List
{607fd4e8-0a03-11d1-ab1d-00c04fc9b304}  CoICOFilter Class
{623E2882-FC0E-11d1-9A77-0000F8756A10}  Gradient
{63A4B1FC-259A-4A5B-8129-A83B8C9E6F4F}  Strips
{649EEC1E-B579-4E8C-BB3B-4997F8426536}  DXTFilterBehavior
{64AB4BB7-111E-11d1-8F79-00C04FC2FBE1}  Microsoft Shell UI Helper
{6A01FDA0-30DF-11d0-B724-00AA006C1A01}  CoSniffStream Class
{6B4ECC4F-16D1-4474-94AB-5A763F2A54AE}  IE Tracking Shell Menu
{6CF9B800-50DB-46B5-9218-EACF07F5E414}  Internet Explorer ETW Collector Service
{6E449686-C509-11CF-AAFA-00AA00B6015C}  Microsoft Active Setup Engine
{6f5bad87-9d5e-459f-bd03-3957407051ca}  IEWindows
{7057e952-bd1b-11d1-8919-00c04fc2c836}  Microsoft DocHost User Interface Handler
{7312498D-E87A-11d1-81E0-0000F87557DB}  Blur
{73CFD649-CD48-4fd8-A272-2070EA56526B}  IE BandProxy
{7658F2A2-0A83-11d2-A484-00C04F8EFB69}  CrStretch
{766BF2AE-D650-11d1-9811-00C04FC31D2E}  HomePage Class
{76F363F2-7E9F-4ED7-A6A7-EE30351B6628}  Inset
{79eac9e0-baf9-11ce-8c82-00aa004ba90b}  URL Moniker
{79eac9e2-baf9-11ce-8c82-00aa004ba90b}  http: Asychronous Pluggable Protocol
Handler
{79eac9e3-baf9-11ce-8c82-00aa004ba90b}  ftp: Asychronous Pluggable Protocol
Handler
{79eac9e5-baf9-11ce-8c82-00aa004ba90b}  https: Asychronous Pluggable Protocol
Handler
{79eac9e6-baf9-11ce-8c82-00aa004ba90b}  mk: Asychronous Pluggable Protocol Handler
{79eac9e7-baf9-11ce-8c82-00aa004ba90b}  file:, local: Asychronous Pluggable
Protocol Handler
{79EAC9F1-BAF9-11CE-8C82-00AA004BA90B}  URLMoniker ProxyStub Factory
{79eac9f2-baf9-11ce-8c82-00aa004ba90b}  Async BindCtx
{7AB36653-1796-484B-BDFA-E74F1DB7C1DC}  Microsoft Spell Checker Factory Class
{7b8a2d94-0ac9-11d1-896c-00c04Fb6bfc4}  Security Manager
{7b8a2d95-0ac9-11d1-896c-00c04Fb6bfc4}  URL Zone Manager
{7BD29E00-76C1-11CF-9DD0-00A0C9034933}  Temporary Internet Files
{7BD29E01-76C1-11CF-9DD0-00A0C9034933}  Temporary Internet Files
{7D559C10-9FE9-11d0-93F7-00AA0059CE02}  Code Download Agent
{7DED4D39-BE20-4AB6-983A-EB4ADCD9C93D}  CLSID_AppRepParm
{7E8BC44E-AEFF-11D1-89C2-00C04FB6BFC4}
{7EE0A24E-A8C6-46ae-A875-8E7C3D18AEAF}  Favorites IFilter
{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB}  WebCheck SyncMgr Handler
{810E402F-056B-11D2-A484-00C04F8EFB69}  CrSlide
{81397204-F51A-4571-8D7B-DC030521AABD}  DXTFilterFactory
{8369AB20-56C9-11D0-94E8-00AA0059CE02}  Cleaner for Downloaded Program Files
{842a1268-6e6a-465c-868f-8bc445b9828f}  JScript Language
{8652CE55-9E80-11D1-9053-00C04FD9189D}  DXRasterizer Class
{871C5380-42A0-1069-A2EA-08002B30309D}
{8856F961-340A-11D0-A96B-00C04FD705A2}  Microsoft Web Browser
{88C6C381-2E85-11D0-94DE-444553540000}  ActiveX Cache Folder
{8A11B5FA-3C92-4E8B-8382-3C71B757D679}  IE RSS Search Protocol Handler
```

Page 12

```
                        SOFTWARE OUTPUT.txt
{8c537469-1ea9-4c85-9947-7e418500cdd4}   ProtectedModeAPI
{8CD34779-9F10-4f9b-ADFB-B3FAEABDAB5A}   .url File Persistent Handler
{8E6E6079-0CB7-11d2-8F10-0000F87ABD16}   Offline Pages Cleaner
{8E989135-2736-4767-8160-EA3613F69D24}   IEDropSourceWrapper
{8fe85d00-4647-40b9-87e4-5eb8a52f4759}   Developer Tools
{93073C40-0BA5-11d2-A484-00C04F8EFB69}   CrInset
{93852550-5403-4E1B-AF8C-5806F151B2F5}   JScript Debugger IDE
{94C00EC1-6E51-447A-87FA-8DF83767C155}   JScript Diagnostic Component
{98FF6D4B-6387-4b0a-8FBD-C5C4BB17B4F8}   IE MRU AutoComplete List
{9a096bb5-9dc3-4d1c-8526-c3cbf991ea4e}   IE RSS Feeds Folder
{9A43A844-0831-11D1-817F-0000F87557DB}   Compositor
{9A4A4A51-FB3A-4F4B-9B57-A2912A289769}   Blinds
{9B0EFD60-F7B0-11D0-BAEF-00C04FC308C9}   Temporary Internet Files Cleaner
{9c7a1728-b694-427a-94a2-a1b2c60f0360}   ShdocvwBroker
{9D958C62-3954-4b44-8FAB-C4670C1DB4C2}   IE Microsoft Shell Folder AutoComplete
List
{9F8E6421-3D9B-11D2-952A-00C04FA34F05}   Glow
{9FAE1230-74AC-4e33-B59C-4051BBEB0803}   IE Thread Handshake
{A1BFB370-5A9F-4429-BB72-B13E2FEAEDEF}   ICMFilter
{A3CCEDF7-2DE2-11D0-86F4-00A0C913F750}   CoPNGFilter Class
{A3DD4F92-658A-410F-84FD-6FBBBEF2FFFE}   Internet Options
{A6B222AB-A5EA-4899-B230-084657EDDC7D}   Browser Thread State
{a7c922a0-a197-4ae4-8fcd-2236bb4cf515}   Microsoft Feeds LoRi Broker
{A7EE7F34-3BD1-427f-9231-F941E9B7E1FE}   DXTFilterCollection
{A860CE50-3910-11d0-86FC-00A0C913F750}   CoDitherToRGB8 Class
{AAC2B978-266D-48ae-AA28-60A3EBB872D0}   IE RSS FeedFolder Tasks
{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE}   Subscription Mgr
{ACA97E00-0C7D-11d2-A484-00C04F8EFB69}   CrSpiral
{ACE52D03-E5CD-4b20-82FF-E71B11BEAE1D}   Shell Name Space ListView
{ADC6CB82-424C-11D2-952A-00C04FA34F05}   Alpha
{ADC6CB86-424C-11D2-952A-00C04FA34F05}   DropShadow
{ADC6CB88-424C-11D2-952A-00C04FA34F05}   Wave
{AE24FDAE-03C6-11D1-8B76-0080C744F389}   Microsoft Scriptlet Component
{AF279B30-86EB-11D1-81BF-0000F87557DB}   Wipe
{B15B8DC0-C7E1-11d0-8680-00AA00BDCB71}   SoftDist
{B31C5FAE-961F-415b-BAF0-E697A5178B94}   IE Microsoft Multiple AutoComplete List
Container
{B3EE7802-8224-4787-A1EA-F0DE16DEABD3}   CheckerBoard
{B54F3741-5B07-11cf-A4B0-00AA004A55E8}   VB Script Language
{B54F3742-5B07-11cf-A4B0-00AA004A55E8}   VB Script Language Authoring
{B54F3743-5B07-11cf-A4B0-00AA004A55E8}   VBScript Language Encoding
{B96F67A2-30C2-47E8-BD85-70A2C948B50F}   GradientWipe
{bdb57ff2-79b9-4205-9447-f5fe85f37312}   Internet Explorer Add-on Installer
{BFAD62EE-9D54-4b2a-BF3B-76F90697BD2A}   IE Shell Rebar BandSite
{BFC880F1-7484-11d0-8309-00AA00B6015C}   Download Site Manager
{C20ED5C4-0A2E-4F66-9BE2-86A1C823DD68}   PSFactoryBuffer
{C21B45B8-5D76-4575-BA27-54823098C491}   IE Microsoft Docking Bar Property Bag
{c2c4f00a-720e-4389-aeb9-e9c4b0d93c6f}   InformationCardElementBehaviorFactory
Class
{c39ee728-d419-4bd4-a3ef-eda059dbd935}   WinInetBroker Class
{C3BDF740-0B58-11d2-A484-00C04F8EFB69}   CrBarn
{c5efd803-50f8-43cd-9ab8-aafc1394c9e0}   IE OpenService Activity Manager
{C6365470-F667-11d1-9067-00C04FD9189D}   Gradient DXSurface
{c6cc0d21-895d-49cc-98f1-d208cd71e047}   Internet Explorer Settings Broker
{C8059EB6-D2FC-4ecf-A15F-AF427F5E4DB6}   Feeds Background Sync
{CFBFAE00-17A6-11D0-99CB-00C04FD64497}   Microsoft Url Search Hook
{D1C5A1E7-CC47-4E32-BDD2-4B3C5FC50AF5}   Slide
{D1FE6762-FC48-11D0-883A-3C8B00C10000}   DXTransformFactory Class
{D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}
{d63c23c5-53e6-48d5-adda-a385b6bb9c7b}   CIEInetcplRasBroker
{DC651A43-0720-4a2b-9971-BD2EF1329A3D}   IE Component Categories conditional cache
daemon
{DD13DE77-D3BA-42D4-B5C6-7745FA4E2D4B}   MotionBlur
```

```
                        SOFTWARE OUTPUT.txt
{DF1E92F3-F333-4EF5-9C38-B75CB65FFC39}   Windows.Globalization
{DF2FCE13-25EC-45bb-9D4C-CECD47C2430C}   cUri
{E2E760C5-BF0D-4241-BFD6-6D0AAB648AC9}   IE WS_Change Notify
{E31E87C4-86EA-4940-9B8A-5BD5D179A737}   RevealTrans
{E48B2549-D510-4A76-8A5F-FC126A6215F0}   CLSID_AntiPhishingBrowserSolution
{E569BDE7-A8DC-47F3-893F-FD2B31B3EEFD}   Browser Application State
{E6E73D20-0C8A-11d2-A484-00C04F8EFB69}   CrZigzag
{E6EE9AAC-F76B-4947-8260-A9F136138E11}   IE Shell Band Site Menu
{E71B4063-3E59-11D2-952A-00C04FA34F05}   Shadow
{E7E4BC40-E76A-11CE-A9BB-00AA004AE837}   Shell DocObject Viewer
{EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}   Microsoft Web Browser Version 1
{EC9BA17D-60B5-462B-A6D8-14B89057E22A}   Barn
{ed72f0d2-b701-4c53-adc3-f2fb59946dd8}   ProtectedModeAPI
{EE0BDDFA-8373-4cc4-85D8-0618E453187C}   IE History Search Protocol Handler
{F088DE73-BDD0-4E3C-81F8-6D32F4FE9D28}   Stretch
{F2CF5485-4E02-4f68-819C-B92DE9277049}   &Links
{F4D36777-EAED-4cc5-9FE7-827BE5190B20}   Microsoft Feeds Scheduler
{F515306D-0156-11d2-81EA-0000F87557DB}   Emboss
{F515306E-0156-11d2-81EA-0000F87557DB}   Engrave
{F5175861-2688-11d0-9C5E-00AA00A45957}   Subscription Folder
{F74B1266-FF39-4B62-8B6B-29C09920852C}   PSFactoryBuffer
{F7F4A1B6-8E87-452f-A2D7-3077F508DBC0}   RandomDissolve
{F83DAC1C-9BB9-4f2b-B619-09819DA81B0E}   IE Registry Tree Options Utility
{F9EFBEC2-4302-11D2-952A-00C04FA34F05}   Light
{faeb54c4-f66f-4806-83a0-805299f5e3ad}   Microsoft Feeds Manager (scripting)
{FBF23B40-E3F0-101B-8488-00AA003E56F8}   Internet Shortcut
{FD7F26E3-9788-4070-BEEC-4EAECBCDDA60}   IE JScript Profiler Core
{FDE7673D-2E19-4145-8376-BBD58C4BC7BA}   IE Custom MRU AutoCompleted List
{FE6B11C3-C72E-4061-86C6-9D163121F229}   Microsoft Feeds Manager
{FF393560-C2A7-11CF-BFF4-444553540000}   History
{ffd90217-f7c2-4434-9ee1-6f1b530db20f}   XML Feed Moniker
Mon Apr 18 15:50:45 2016 Z
{10072CEC-8CC1-11D1-986E-00A0C955B42E}   PeerDraw Class
{17FE9752-0B5A-4665-84CD-569794602F5C}
{C5621364-87CC-4731-8947-929CAE75323E}   PSFactoryBuffer
{D6FCA954-F7AE-4EAC-8783-85F5E4ABD840}   PSFactoryBuffer
{DF4FCC34-067A-4E0A-8352-4A1A5095346E}
Mon Apr 18 15:45:53 2016 Z
{1118F681-7218-4071-B478-90D898A7663A}   FolderView General Property Page
{338A89AA-7C3B-4581-884B-C83D330B793B}   WXFD2P.WXFD2PService
{4E3770F4-1937-4F05-B9A2-959BE7321909}   WZShellViewControls.TreeNode.61
{5F5EAFCF-CBE1-49F6-9489-9308BB6B5D8F}   FolderView Property Page
{7DD84CCA-FCB2-4D18-A01A-C19E031176CF}   FileView Property Page
{A09AE68F-B14D-43ED-B713-BA413F034904}   Sky Software FileView ActiveX Control 6.1
{E0D79304-84BE-11CE-9641-444553540000}   WinZip
{E0D79305-84BE-11CE-9641-444553540000}   WinZip
{E0D79306-84BE-11CE-9641-444553540000}   WinZip
{E0D79307-84BE-11CE-9641-444553540000}   WinZip
{E0D7930A-84BE-11CE-9641-444553540002}   WinZip Preview Handler
{E5EEF3A5-0D17-4251-93B8-D9BA39105C55}   WXFWMRK.WXFWMRKService
{F3834A2B-19CF-4A90-BE1D-ECC410D9DA09}   Sky Software FolderView ActiveX Control
6.1
{FE05A222-0875-42E6-896E-EE3851326361}   Special
Mon Apr 18 15:45:34 2016 Z
{2A450F8D-D083-45A8-B927-DB08431C79AA}   ScDataCache Class
{4E03B17B-A537-4EC2-B39D-F1F6E2E929C9}   DataSharedStore Class
{5E248397-8614-4EC5-8926-BD242DC9830A}   EventNotifier Class
{6AB3EB99-B2F7-4950-BA33-954E286E424C}   ac.sharedstore ID lookup
{E78ED05C-EC93-40E7-BC13-E1D7A9FBEDE0}   PINSharedStore Class
{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}   Subscriber Class
Mon Apr 18 15:44:55 2016 Z
{058D42F2-DBB1-11D6-B856-00C04FC06913}   AdobePDFMakerX.VisioLayerDlg
{0B5DB071-ABF4-49D4-B67A-3956DDEFFAFB}   SecuritySettings Class
                              Page 14
```

SOFTWARE OUTPUT.txt
```
{0CD1257A-50DD-48C4-BCB0-74B52EB054CF}   AdobePDFMakerX.AcadBatch
{0F97F1EF-7C1A-45A8-B951-65B00D039116}   AdobePDFMakerX.CustomPropertyDlg
{178687A2-ABF5-43EE-AEF6-B380D8A9FD7C}   PDFMakerApp Class
{1A348363-F970-4871-9E43-AA777D4A5488}   AdobePDFMakerX.EMailProgressDlg
{1CDE2E84-991C-4BFC-8A31-AA52C1CF71E7}   AdobePDFMakerX.AcadBatchProgress
{2065DA61-FBD0-11D6-B862-00C04FC06913}   AdobePDFMakerX.ConvertAttachError
{20AA230C-5224-451E-B8C0-37F261DD5F4A}   AdobePDFMakerX.ApplicationInfo
{21F11D95-031D-4403-9856-80834DF94B59}   AdobePDFMakerX.SimpleStatusDlg
{29405572-43FB-11D2-9758-0060979C3633}   AdobePDFMakerX.Word
{2E1F500A-DE74-4452-A018-E0A080ECF5A1}   AdobePDFMakerX.AccessBadRptDlg
{36C3DCDD-2525-40C6-BAE9-6507DD3DA8C2}   AdobePDFMakerX.CustomYesNoDontAskDlg
{545B74BF-B996-43CF-9C88-111D55E6E610}   AdobePDFMakerX.MailBoxDlg
{5789D319-A0E6-4788-8120-B0D3D1AB9797}   Acrobat PDFMaker Office COM Addin
{5F2F8074-C34B-4AFF-B218-6C69399F6CDC}   AdobePDFMakerX.AcadComments
{66BD7D2F-1227-47D3-B613-C3968AAABC56}   AdobePDFMakerX.OutlookGuardianSummary
{7C4D2F80-790E-11D6-82C7-00C04FCFC84E}   AdobePDFMakerX.DialogImportComments
{7F2AB156-ABE7-48A1-A581-350BE149D414}   AdobePDFMakerX.ConversionOptionDlg
{838186E3-56E1-11D2-9758-0060979C3633}   AdobePDFMakerX.WordStatusDlg
{897D7B50-2CB6-4E43-B07C-768B2F2B9457}   AdobePDFMakerX.ExcelSheetsDlg
{9177B23F-7D46-11D6-B816-00C04FC06913}   Acrobat PDFMaker Office COM Addin
{BAAB3B02-59D7-4C24-A44A-D9A0A24E6BED}   AdobePDFMakerX.OutlookGuardianPolicies
{BE74BD18-D040-4A19-85CF-21E5BDF6B2F0}
AdobePDFMakerX.OutlookGuardianFileSelection
{BF8230FC-439A-4CDA-857B-7118F27BD396}   AdobePDFMakerX.TranscoderOptionsDlg
{CF8187B6-14B1-49E3-A4AB-000B944FA0A2}   ConversionSettings Class
{D1530EB4-BAAA-43D1-9007-FC9FA29C6212}   AdobePDFMakerX.EmailArchiveDlg
{DC6A2437-8992-4E85-8081-DC92C93C0075}   AdobePDFMakerX.LayerDlg
{E69CBA0B-3B2B-4657-8835-92BCAF53EE17}   PDFMakerDriver Class
{E6BE6A45-8093-462C-AF3B-8E77BA265A36}   AdobePDFMakerX.AccessReportDlg
{E715BF17-A559-4F3B-888F-7632354BDD24}   AdobePDFMakerX.LayoutDlg
{EEA07F81-E5A5-11D6-B85A-00C04FC06913}   AdobePDFMakerX.PDFConversionProg
Mon Apr 18 15:44:51 2016 Z
{D25B2CAB-8A9A-4517-A9B2-CB5F68A5A802}   Acrobat Elements Context Menu
Mon Apr 18 15:43:15 2016 Z
{4E9963B7-B2BF-4685-9378-8FEBEA364EF8}   Microsoft.Aspnet.Snapin.About
{5437FDFA-9EC9-4CCC-8531-42F8D9C19AF7}
Microsoft.Aspnet.Snapin.AspNetManagementUtility.4
{59856830-3ECB-4D29-9CFE-DDD0F74B96A2}
{F4E1E7F6-A035-41B3-9856-A3C3A1C4684F}   WCF/COM+ Integration Service Moniker 40
Mon Apr 18 15:42:14 2016 Z
{07B0E5E9-D635-4CD3-B98D-7C10E700DEA0}   PimcSurrogate Class
{2A7B042D-578A-4366-9A3D-154C0498458E}
System.Management.Instrumentation.ManagedCommonProvider
{45FB4600-E6E8-4928-B25E-50476FF79425}   Com Call Wrapper Unmarshal Class 4.0
{AF44BF80-36DD-4118-B4CF-8B1E3F4FB9CE}   PSFactoryBuffer
{BFFECCA7-4069-49F9-B5AB-7CCBB078ED91}
System.ServiceModel.Internal.TransactionBridge
{E23B1CED-5E47-4FDB-AF66-B20370261B5E}   PimcManager Class
Mon Apr 18 15:37:36 2016 Z
{9F550240-0FCA-443D-B5E9-23ACB47F62E2}   DLAutoMap Class
Mon Apr 18 15:31:09 2016 Z
{07EA4705-27AB-4BE4-84EB-5806CF3F381F}   PSFactoryBuffer
{0B114A3B-3521-4486-ABEB-87FF1902C6F8}   PSFactoryBuffer
{0BA98CA9-BB63-4A42-B224-F18486A81E9E}   PSFactoryBuffer
{41D4800E-FF3C-11DC-AB6D-18A956D89593}   PSFactoryBuffer
{4B2C3F29-D0A8-4B33-B23E-A83B642B94A3}   PSFactoryBuffer
{7C28E9C9-9880-48EB-8E7F-B74552690F6C}   PSFactoryBuffer
{8D6CD264-C426-4CD0-A00A-975618A6886B}   PSFactoryBuffer
{B3534612-4287-4109-8691-765A5B57F565}   PSFactoryBuffer
{B620001A-C73C-4448-8115-A997F69B1E28}   PSFactoryBuffer
{BCD59196-43FA-44B5-A3F6-BA6CAAAF9E9C}   PSFactoryBuffer
{D27FA62F-F4A1-48E3-8A6D-D9BAF51D4457}   PSFactoryBuffer
{FA75662E-C260-443F-A836-71537C714CC1}   PSFactoryBuffer
```
Page 15

SOFTWARE OUTPUT.txt
Mon Apr 18 15:31:08 2016 Z
    {18371B04-57EC-472D-AAFC-8F995D6D8E18}  PSFactoryBuffer
    {2A26885D-0A56-4BC6-A4B7-080488DBD52D}  PSFactoryBuffer
    {2C66DE3D-C2DF-417C-B11F-D76B7EB0CF42}  PSFactoryBuffer
    {40F3B4A5-E0C8-49F4-8FFB-21DC8E1D3DEE}  PSFactoryBuffer
    {41A99C09-1ED6-49C6-974B-7149AE0D22A4}  PSFactoryBuffer
    {6FE6BA00-BF79-45A5-BE1B-9E723094BFED}  PSFactoryBuffer
    {72B1C3CF-A717-4F08-AEBE-143F1A9E3FF0}  PSFactoryBuffer
    {81E90B00-DF87-4852-ADC5-0147EC22325A}  PSFactoryBuffer
    {8DDCFB00-1D1A-4CC4-BE3F-CF4F7C6444B6}  PSFactoryBuffer
    {95127615-453C-46DE-8350-1E647D2F113F}  PSFactoryBuffer
    {9946AF19-3E43-4A13-B4C0-55D8F8AC8E96}  PSFactoryBuffer
    {ADCB85F4-72AA-424B-A12D-D2503F473226}  PSFactoryBuffer
    {D535C884-6B82-47DD-9A15-09E98B95136E}  PSFactoryBuffer
    {DA46DD8F-A388-4001-A127-12E6D8B1F634}  PSFactoryBuffer
    {DF69F800-A084-43C3-B7B9-99AB16CEEEE2}  PSFactoryBuffer
    {F2E16B2E-171F-4B06-8E4E-4F8344E81812}  PSFactoryBuffer
Mon Apr 18 15:30:46 2016 Z
    {12F246F3-DF68-4252-AE6B-07B9CF73B99A}  Local Policy Authority Document Store
Provider Class
    {31FA1CB7-9F17-4C81-A6FF-D75AD89B2F41}  Environment Class
    {3AFEA1D5-6518-4BE3-B12D-ED3325DF0515}  PolicyProcessorProvider Class
    {A6A2160C-40DB-4EAA-AF21-6FDEA46E10B1}  FileFolder Class
    {CB8C9686-05E7-471A-93D4-AD187B572701}  RegistryProvider Class
    {D3AAFEF2-42B0-43B3-98F0-75FC7AEE11F2}  AppInfo Class
Mon Apr 18 15:28:51 2016 Z
    {047ea9a0-93bb-415f-a1c3-d7aeb3dd5087}
Mon Apr 18 15:28:47 2016 Z
    {00E80F18-EC5B-4FCF-A417-7348991A8D32}  Stereoscopic3DSettings Class
    {01367108-5EE2-4E1C-A8DE-24438065ABC9}  CategoryAppearance Class
    {01504157-8839-4BF6-9B5B-51165A967B2B}  MainServer Class
    {055A7699-EAFF-47DF-8E55-41F4C0612BF3}  VideoColorSettings Class
    {07333BBD-64AF-4206-899D-2809660C61C7}  ECCSettings Class
    {074BFFFD-4E50-42c1-A7EB-40D9D70F2471}  AdjustDesktopSizePos Class
    {0EEC1AF6-7664-4D17-88A5-B71EF18A93BC}  MainServer Class
    {0FB41BD0-3107-40A5-8D49-456E585947B2}  IdentifyDisp Class
    {1618348E-35B3-4631-8C04-2AB15AF5007D}  SetupMosaicEx Class
    {1BC39379-8D90-4F18-8817-795C57163770}  ScreenMove Class
    {1DC715B2-9126-4671-8086-299A44543E0F}  NvXDBatchEngine Class
    {26A37DC6-935D-439B-80DD-C1006AE13D71}  Config Class
    {294EC7E3-94B7-4A6C-8636-09B33674D58F}  Panoramic Class
    {2DF0ACC2-6D97-491b-9581-70A6001FD25A}  GamesCompatibility Class
    {2FD96798-0D65-4D57-A095-B57679740E37}  CategoryPerformance Class
    {3020E6D8-7D1A-4D3C-8B62-C4D4B8F28434}  Category_Video Class
    {3156EC84-29BD-4EAA-AE0A-817ED606FA99}  MainServer Class
    {33C89616-F807-4957-BF34-A1C91D7A1A2E}  OperationInterceptor Class
    {3D1975AF-48C6-4f8e-A182-AC5012248AB5}  NVIDIA Play On My TV Context Menu
Extension
    {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9}  NVIDIA CPL Context Menu Extension
    {3E500C0C-5D15-4610-8095-7CEBD4C43F24}  MainServer Class
    {49E6B51C-DB5F-4178-8691-412463C1A0EB}  PipelineRegistrar Class
    {49F585C0-CE12-4306-9100-B6A28857B10B}  CustomRez Class
    {4FC7F090-041C-4730-BD24-AF4BA8A2A5E0}  NvXDSerializer Class
    {50125552-EC89-4049-B1B7-5FDBE38C8509}  SetUpStereoVision Class
    {5135A9C0-F05A-4FBD-8EC6-6B920CD387F6}  TopologyViewer Class
    {51840041-B26F-4843-B358-22ABB067396C}  ScreenTimingDVI Class
    {5387A36B-6F55-4C66-B085-E18393FCEA87}  StateDataSessionFilter Class
    {54CEE07E-E1C8-45DB-B550-417E75C4CA58}  TopologyViewerVista Class
    {56CDA654-2AA2-456F-81B1-153FE7B381A2}  PowerMizer Class
    {5DF4E7C5-78E3-4CCA-93CD-DF1639E165FB}  NvApixEngine Class
    {6017A978-93AD-4F2F-9E2D-07CF8C8DEBC4}  RotateDisplay Class
    {63005CD0-8541-439c-A66A-617F4B1F2BCB}  TVSizeMove Class
    {6539579C-2657-45E5-985F-835E197959C2}  AdjustSizePosExt Class
                              Page 16

```
                        SOFTWARE OUTPUT.txt
{6A10CEAB-0813-48BA-9769-BD98F03F3EB8}   SynchronizeDisplays Class
{6A22E68F-887C-4221-9DF1-EE0B3AC76497}   NameDisp Class
{6E4B938E-4BA1-4E8D-BCBA-8C51CE95F94F}   MultiMon Class
{6F3F133D-61E3-4153-8AAE-056031E2B597}   FullScreenVideo Class
{7112FB6A-700C-4C25-BB31-5B13CE60CC29}   SmartDimmer Class
{73BCA54E-6AEB-4597-8F27-E1284FF12722}   ServerMain Class
{75BDD7A1-1224-41DA-90B4-457ACD874F12}   CategorySDI Class
{7735B86B-2EAB-43EF-B5DE-31A15F767C14}   SDISettings Class
{7945F814-7BFB-4506-A113-2BD66CDC713A}   DualView Class
{7BB17C5A-3176-4B40-A3F9-39D4A64D7E83}   CategoryGfxSys Class
{80BA3813-908F-4D4C-A5FF-263640AD5B7A}   VariableRefreshRate Class
{81667C73-F396-44a3-923B-3749C0840A58}   TVHDMIColor Class
{86193C76-0DCA-4B33-83CA-6D7DCCA48D0B}   FSSettings Class
{87CDE238-C2D9-4E31-99D7-DCD6A7E15F19}   TVImage Class
{88FC94D1-2ABB-42CF-8A07-4BC54F66EDDF}   CategoryMultiMon Class
{894BF76C-115F-44B7-9B32-ABFA7E6A804A}   MultiView Class
{89B53798-9A96-4758-9571-93B72CAA5381}   TVFormat Class
{91363F1E-E7CA-4959-85D6-963719EC79FC}   ChangeResExt Class
{9B0C8B3B-8CA5-46cb-B0DD-64542BBA21DC}   Overlap Class
{9B5EC720-9A44-4811-8B9F-24BD53F2050D}   AppSettingsBasic Class
{9BC49CE1-EFA7-4C49-8BB2-5355FEA6C170}   ManageMaximusSettings Class
{9C1878FA-A0CB-4F01-8762-A6BF18021C94}   SetupMosaic Class
{9C7684B5-FC31-4e57-A852-282D907911CC}   Category_Video Class
{A158544D-66FA-4F19-8806-F3CA2E2A4C52}   Power Class
{A3B877C7-83CA-4c9b-87FB-BE0D518C2441}   SetupDigitalAudio Class
{A4A74456-67F8-4F18-B96B-0F1F05DEF65A}   CateogryPowerManagement Class
{A70C977A-BF00-412C-90B7-034C51DA2439}   DesktopContext Class
{A8679087-E64A-413A-9CBF-F38BE510C46C}   Cat1 Class
{A929C4CE-FD36-4270-B4F5-34ECAC5BD63C}   NvAppShExt Class
{AAB8F985-EADA-428B-8636-270F58E1F1EF}   VideoAudioControl Class
{AD374A9E-D7FC-453A-A146-16535FE9ECC1}   NvXDPlcyEngine Class
{B53EBC0C-2251-4AE2-9818-FD6AAF843EC2}   ColorSettingsAdv Class
{BBB7D605-8639-49D0-849E-32C4A5DBB9C3}   Manage3DSettings Class
{C4A29158-1A7E-425f-B25E-80FA382AAA14}   MainServer Class
{C8F113AE-A2C9-47CB-8DAE-9376C64665AD}   SliPhysXExt Class
{CC0648AE-7E85-483C-B1DB-9335C9D6F8C7}   ColorCorrection Class
{D385E909-3F89-4ECD-B38F-AC11F9FE6F1C}   VideoZoom Class
{D474EBC0-2851-4389-893D-030D2B6BCED1}   TopologyViewerEx Class
{D8A8B20F-98D2-4EFF-8CE1-EF094F1A8043}   CategoryFS Class
{DCAB0989-1301-4319-BE5F-ADE89F88581C}   SyncProxy Class
{DDEF97F5-723E-47D2-87B1-14C39EFBAE11}   ManageSdiOutput Class
{DE0549BD-F34D-4748-AD94-0F2F22749F4F}   SliBasic Class
{E851CB66-C839-4E96-8363-8535EB16FE2C}   SmartPower Class
{E97DEC16-A50D-49bb-AE24-CF682282E08D}   OpenGLShExt Class
{EDAC9CAA-4874-48C0-80DB-2D81B63EFE13}   TVSizeMove Class
{EEF5290C-7F3D-4640-93F2-F189DC616510}   VideoHDCPStatus Class
{EF884939-F1EA-4EFB-B676-D2F802177C5F}   VideoImageSettings Class
{FC7AA68D-EAFB-4ce9-A012-9C33E7B02B49}   ManageQuadroPlex Class
Mon Apr 18 15:28:46 2016 Z
{87BDED91-3F10-4383-B8C1-26886F49F141}   NvXDSyncEngine Class
Mon Apr 18 15:28:07 2016 Z
{048E5288-25FF-4552-BFE0-A9B7DE629CBA}   DsrApi Class
{073E187F-BB72-4d0f-8368-C6A20CD9EA50}   ForteProcModeApi Class
{0803F79D-A6CB-42F1-A46C-A1B0F067FEFC}   DaisyWrapMFX Class
{0CC838CF-95B2-42cd-BED1-324E39134692}   CTAPOContainerGFX Class
{0E249A19-94DF-418A-9191-41D1FA0F3C2E}   RtkApoNotification Class
{0F62DFB3-DB5B-458D-9371-6B45C4582560}   CTAPOContainerSFX Class
{10E241D3-EA1B-4edf-BFB5-61B7055C9DF0}   DtsApoBtPage Class
{11825B7C-5AA6-4E2F-A4BC-67659568E925}   SRSPremiumSound Class
{130D6967-A060-4231-892A-933475EE2CB2}   SrsLaunchPage Class
{17AB05B2-E3B4-43FE-885B-06B84E251E5D}   CTAPOContainerEFX Class
{17e73a4b-89c0-4b3f-b7a4-183cfed234a6}   CTAPOContainerLFX Class
{19d68d4e-5e29-41d4-bde0-aaafeb930b20}   CEffectNodeInfo Class
```

Page 17

SOFTWARE OUTPUT.txt

```
{1D1708DE-F500-4402-92ED-5CA693DABE72}   DLitePageHDMI Class
{22220001-5ee5-4a88-9c52-cc2989d6ac6d}   MaxxVoiceAPO Dock Class
{22222283-f501-4114-a51f-04b318d992e4}   MaxxVoiceAPOLFX Class
{248F37DE-5F40-4dc6-9B51-3A14C1D71FD5}   DPCEE3RApi Class
{24A06156-8EC3-4d0b-85D1-41CB0831DA1C}   XearPage Class
{25f1de92-f75b-4ef5-b52f-1a6549182286}   CTAPOContainerGFX Class
{30CB44E2-8BC1-44bd-A6DD-2E58E2365CC8}   DtsApoConnectPage Class
{31929B1C-6E3C-431c-A20D-2A2A8315344D}   RtkRecOptionsApi Class
{31A53A7B-E0D8-4f99-B950-F6C8F25E6731}   AdvEndpointPropPage Class
{33330000-3657-4da7-96d6-9c0808ca95a6}   MaxxVoiceAPOPSS Class
{33330001-fcfc-4367-9e0e-5d4533ff7dcb}   MaxxVoiceAPO Dock Class
{33333337-c9bd-47cd-8a2d-de4341773869}   MaxxVoiceAPOLFX Class
{38361248-B055-4ea8-A373-940464FB318E}   SAApi Class
{3A2B839D-6060-4711-B3A8-35132A881E78}   DPCEE3Api Class
{3A40ED31-B1EB-4905-8A9A-7B65F78541BE}   RtkCapVoicePage Class
{42D0571B-9239-4eee-B8A0-1C8B85608894}   DTSUP2Api Class
{42F7121A-9917-4927-9E44-C9B305B0EDBB}   RtkSRSPSApi Class
{43306DF8-E185-415d-BA78-D50E337921FA}   ForteRenderPage Class
{43B6893E-1071-432B-968E-DD683ADA6589}   AndreaPropPage Class
{44440000-c661-4f31-a1a4-94937c15c087}   MaxxAudioAPO B Class
{44444440-42ce-433f-9992-8eb7976b907b}   MaxxAudioAPO Class
{44EE5F71-5DD2-4434-B1AA-16B850F4BEC5}   SounzVoizApi Class
{45750165-6E3D-4413-AEE0-D486BC169E0B}   TAdeApi Class
{46D50ACF-34CA-4dfd-ACC8-481F6E686936}   Rtk3DHpPage Class
{498A0C2A-D4C5-4cbb-B62F-FB075A02F5A8}   MCEQApi Class
{53641EC4-4566-4896-919A-2FBB21FD2FCF}   DaisyWrapGFX Class
{55550001-9c76-457f-b3d2-a1400b696958}   MaxxAudioAPO Dock A Class
{55550002-a639-4dc2-b816-21158f7cb9ed}   MaxxAudioAPO Dock B Class
{55550017-0c8d-4bac-baf2-24ac14b873e2}   MaxxAudioAPO B Class
{55555548-68cc-4cd7-b0b1-e5744039e781}   MaxxAudioAPO Class
{5680B311-447E-4fb6-B327-3C9B50A56FE3}   CEPage Class
{5860E1C5-F95C-4a7a-8EC8-8AEF24F379A1}   CplPage Class
{5B05A596-33CA-4D65-B6C8-42704CA9BE2A}   MaxxAudioApi Class
{5DE0635D-0C4A-4651-B00F-A1A87A2A5BBF}   DolbyPropPage Class
{5F4F9B2A-5992-4005-9714-021EBC439E9A}   DtsApoSyPage Class
{6147b7f5-1bb4-4117-b0d9-ada799329479}   CTAPOContainerLFX Class
{625B52E8-3C5F-4d1c-ABD3-DD8E4526F059}   CTAPOContainerLFX Class
{62AF1550-7402-42c2-8B94-9C644780F3AC}   SF3LinkPage Class
{62dc1a93-ae24-464c-a43e-452f824c4250}   WM LFX APO
{637c490d-eee3-4c0a-973f-371958802da2}   WM GFX APO
{66660000-626b-4aea-b582-5895aeddf39f}   MaxxAudioAPO B Class
{66660001-81f3-42cd-9a32-5c72273431fe}   MaxxAudioAPO Dock A Class
{66660002-06d0-4b9d-a121-775aa4ac208f}   MaxxAudioAPO Dock B Class
{666666de-de1f-47e6-a4c4-dba360675157}   MaxxAudioAPO Class
{6861CFDC-0461-49d5-A8DF-BE5ACD02692F}   RtkAdvPropPage Class
{68E6DF30-3484-489b-8120-3C4C0256A758}   RtkApoCommonApi Class
{697A25AB-7233-4E22-A6AB-896387D1980F}   ABIT Class
{6A25A050-525C-4c97-A072-9504F8E8E77D}   ControllerPropPageLoader Class
{6DECA3ED-3EEB-4ebd-8255-74686F53D707}   SoundAlivePage Class
{6FC60FF9-EDBB-47B5-9496-05D00561EF4B}   ExtDspPropPage Class
{71833FDE-B66B-44aa-8993-5512920C1B4F}   Knowles2Page Class
{727120C0-5689-4e6d-AFC0-E9762ABC32B8}   MaxxAudioPage Class
{72DA76A6-046C-4f1b-B7DD-4595A5ECF375}   DolbySPage Class
{735CBF5A-7149-4d58-B35C-AFE4862A2311}   DtsApoUpcPage Class
{74C7569D-ED69-4292-9886-CC89DD455744}   PropPageStub Class
{7505CB57-3A77-46a4-8B04-75897B0AA643}   RtkOmniSoundApi Class
{7A84CB1C-5B82-4999-B028-D19EA3004D77}   RtkAM3DApi Class
{7ECCA61E-6028-4afa-B03C-B68004412CAF}   RtkBassBackApi Class
{801F7DFC-E551-4E01-9CAF-29BFC339984E}   DaisyWrapEFX Class
{818D2D10-8A8C-4270-B044-AF1A5759D73C}   RtkRenderNsPage Class
{853B15F2-A9DE-4592-9FA9-7A69F6AEA6A2}   DPCEE4Api Class
{8852ECE8-595D-427E-B5A0-F8D2E62FABBD}   SrsApoPropPage Class
{88A0B959-0AAC-486e-90EC-90444C40F7EC}   RtkRecNoLimitApi Class
```

Page 18

SOFTWARE OUTPUT.txt

```
{8E93A1B1-8EF0-42e9-AC76-D2CA4CF28681}  OptPCEE3Prop Class
{93EC11E9-889B-458e-8DEE-B750C8AAC6C2}  RtApocapsApi Class
{9914A841-B21A-489C-949C-89306F33BF9A}  DSpruseApi Class
{9C4B415C-B076-43F4-928D-98D8B465087A}  DtsS2UltraPcApi Class
{9D1C81FD-A77A-4cc0-BD6E-A827C9E38ACA}  MaxxAudio3Api Class
{A5A63314-41AC-484F-85B8-FC15335C24CF}  RtUpDownMixApi Class
{A6CB57B4-E35B-4ddd-BC32-CA3D4479079D}  DolbySprucePage Class
{A9C2CEBF-36DC-40A3-92E6-ED59FDD9D20D}  SONY Class
{AAF1A9FE-267c-4528-ADFE-F34397B99B6D}  MaxxAudioAPO Class
{AD7476AF-BE9F-409a-9A66-FFD991FEC6D2}  RtkClrRecPage Class
{AF099A7C-45D2-4CE6-9327-EEAAB0395444}  RtkCfgApi Class
{B4928187-D2E3-4CFA-A2C2-A9C97B4956EA}  DmsApi Class
{B786AA8A-3748-4cf4-9F64-F4077DA25F0F}  OptPCEE3Prop Class
{BC1F9ACF-DCA1-43d4-AFEE-D742DC11473C}  RtkRecEffectsApi Class
{C26C3384-7112-4b5a-8BB5-1328D9543D79}  SonyApi Class
{C4686FF2-11A2-4e2e-A670-AAF1E8B295B4}  AndreaRenderPage Class
{C51686E8-256E-4bee-9A7A-08A55C48A718}  BbePropPage Class
{C6606CA5-2108-4CAF-8E52-1953F2DBF716}  PropSet Class
{C69FE6AD-9AA8-45DE-BA75-C72117B21C07}  CTAPOContainerMFX Class
{C8197EBA-2423-43ed-B9E6-D8C63B928D5A}  DTSU2PPage Class
{CC0CA09A-5B84-43F2-BE5C-9169C192565F}  RTLCSSAPI Class
{CE93F536-D2FB-4e8f-8193-F57AD8BC90D5}  DTSPSApi Class
{d0d09f5b-08dd-4619-aa88-dc9cd2e794d1}  CEffectNodeInfo Class
{D4A1C23B-049F-44f6-8CE0-8173614AAC9A}  KnowlesPage Class
{D8813D24-E801-4a75-9985-30E7CC9DBD93}  DaisyWrapLFX Class
{D9A965B0-0278-4972-B82E-299F34FC0B54}  SrsPropPage Class
{DDCFD625-B4EA-4528-AC09-39D695027AC4}  ConexantPage Class
{E0760680-E3E3-41A6-A5BE-275F5C21BDD9}  DPCEE3sApi Class
{E4D7C1C8-9459-45f8-A541-CE54DE835DD5}  RtkUtilApi Class
{E51EF0ED-35D5-4bde-93E9-28CA62B1E704}  MDRCApi Class
{E650330C-4082-462b-ABAF-B0F9F2F542B3}  CEffectNodeInfo Class
{E9A2EE74-9791-4dc6-9066-D7D908C6C613}  DtsS2PropPage Class
{E9F1F599-7B14-4213-BF46-F992758CAB81}  RtlCP Class
{EE4B528E-5C11-4f80-BCA3-C88647061D79}  DTSConnectPage Class
{F2464A7E-5B09-4199-826F-7D6A16AF2E59}  RtkWavesApi Class
{F2725209-D040-48ba-B5B3-FAE9060BC3C9}  EndpointPropPageLoader Class
{F59167DD-ED87-4f6c-843D-33219D584756}  SrsDisablePage Class
{F841F354-41AB-4652-81EF-F879AE87F9FC}  DaisyWrapSFX Class
{FB6AE33C-D9B6-4b09-8DF1-AE7AAD5C9530}  DolbyPCEE3sPage Class
{fe512d41-3f30-4442-b5df-7889cb2aad7a}  CTAPOContainerGFX Class
{FF894E2A-5C73-4b58-838B-81958856CFB5}  DtsApoUpcSyBtPage Class
Mon Apr 18 15:28:06 2016 Z
{30543F69-1213-4284-9D0A-5CE5F71A82CD}  DhtApi Class
{3739576F-F27B-4857-9E3E-8BAAA2A030B9}  RtNuanceProc Class
{6201C0B0-A1DC-4AE2-9665-8DAB2E380073}  DolbyApi Class
{9F39C0AE-979D-4BFC-890D-4BDF6FD7BDE1}  DDLiveApi Class
{A27368B3-D810-42ce-B114-83900258B8EC}  RtkAPOGFX Class
{A296D363-EE83-4af9-9BE7-729C1296150A}  RtkAPOMFX Class
{A29EB043-6CE2-4ee2-B38C-F58719E0D88F}  RtkAPOEFX Class
{A51A19D6-80F1-4abf-AB95-AF5215E8B052}  RtkRecLFX Class
{A69C91DC-11C4-414f-A919-4DA8EA3F3CA6}  RtkRecMFX Class
{A6EDD1A5-1ACA-4110-9B21-AD7EDC210CA3}  RtkRecSFX Class
{AB3B404A-B18F-4b4f-B91F-77F2DE95EB18}  RtkRecEFX Class
{BBA39DEF-B0D8-4D50-9133-85D5B1AC7971}  RtDataProc Class
{DA2C9ECE-7418-4906-B4FA-0A00B3EB88AA}  RtkAPOSFX Class
{DC253AB8-10DC-483c-AB5F-D6A4E189FD70}  RtkAPOLFX Class
Mon Apr 18 15:28:01 2016 Z
{DC09760E-9FDA-454A-B9D2-7E663E58C39D}  PSFactoryBuffer
Mon Apr 18 15:28:00 2016 Z
{0bbca823-e77d-419e-9a44-5adec2c8eeb0}  NVIDIA Control Panel
Mon Apr 18 15:27:47 2016 Z
{FFB699E0-306A-11d3-8BD1-00104B6F7516}  NVIDIA CPL Extension
Mon Apr 18 15:27:42 2016 Z
```

Page 19

```
                          SOFTWARE OUTPUT.txt
    {7F5B8FA4-BEEC-11cf-9BD7-B76592786C03}  Dell Touchpad
    {D0B6E6C2-3485-42E8-A26E-3E3735B240B6}
Mon Apr 18 15:27:21 2016 Z
    {059A5BAE-5D7A-4C5E-8F7A-BFD57D1D6AAA}  Intel® Hardware VC-1 Decoder MFT
    {071BCD17-1720-430B-AB8B-D6E4AB56689F}  TheIntelSmartFrame Class
    {223A2D27-0448-4247-B4AC-DE846A23C71E}  DriverInterface Class
    {27E7234F-429F-4787-AC8F-8AADDED01355}  PSFactoryBuffer
    {280A8F40-E382-11D2-B561-00A0C92E6848}  Software\Intel\Display\igfxcui
    {45244F59-BE44-45D2-8B67-C8D4FE270EB6}  TheLaunchTimeEnhancer Class
    {45E5CE07-5AC7-4509-94E9-62DB27CF8F96}  Intel® Hardware H.264 Decoder MFT
    {4BE8D3C0-0515-4A37-AD55-E4BAE19AF471}  Intel® Quick Sync Video H.264 Encoder MFT
    {81719F80-8503-4AA6-99F6-EDD8353B6CD4}  DPTopologyInt Class
    {9B5F5829-A529-4B12-814A-E81BCB8D93FC}  TheDeskTopContextMenu Class
    {A8CB24B9-7B0B-462F-A2B7-48746020A43D}  CUIString Class
    {CD5BA7FF-9071-40E9-A462-8DC5152B1776}  Intel® Hardware MPEG-2 Decoder MFT
    {D5F5053A-9585-4D80-8F6F-7B6587CEFB93}  DataHandler Class
    {EE69B504-1CBF-4EA6-8137-BB10F806B014}  Intel® Hardware Preprocessing MFT
    {FA507C3F-30C6-4DCA-9EE5-2656072EEC14}  TheAdvOSPropPage Class
Mon Apr 18 15:26:53 2016 Z
    {311C1772-ED67-4fdf-BC5C-7EF1342FE9A5}  DmDragDrop Class
    {95126314-DA62-48D7-836B-D70F9CB15FC7}  DmRteSpellChecker Class
    {C98AAA6B-FBAC-4FE5-A815-0D3A4176DA64}  Utility Class
Wed Dec 30 12:23:06 2015 Z
    {4FF4E346-45F7-4823-A7FB-8A8D5FF285F8}  PSFactoryBuffer
Wed Dec 30 12:22:11 2015 Z
    {08049768-774A-4B91-8B39-87FFBB2BF28E}  SKI Class
    {2E03C01D-D9A2-419D-BF56-FCFDA14FF879}  PINAccessor Class
    {38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}  Card Class
    {7030D479-1A29-4935-8B42-B4B619992DFF}  ReaderManager Class
    {8F5330A7-4214-45F4-8736-0ED72C96DEB0}  CardAccessor Class
    {A082D824-693A-47D0-832A-918F160F839F}  Reader Class
    {BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}  SDKCardServiceFactory Class
Wed Dec 30 12:22:10 2015 Z
    {05EEE5A9-F903-4D54-999C-A43C547EF034}  PSFactoryBuffer
    {070695CD-CB20-4254-B3EF-6D89228DE220}  PIVInterface Class
    {0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}  StaticAccessor Class
    {0D77058D-09A6-4D40-B3C2-FDBA8E77288B}  ACStatic Class
    {190E1E02-263E-4CF5-8978-F6B5838E0090}  SmartCardConnection Class
    {193795BC-B81F-4900-B391-349EA9019C0F}  PSFactoryBuffer
    {1C1451BA-4F87-4944-8111-5E4078C87C87}  SKILogicalCriteria Class
    {2599E050-87CD-49F0-9A49-92DAED39D313}  PSFactoryBuffer
    {30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}  BSI21 Class
    {46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}  StaticLogicalCriteria Class
    {5B985AAD-0DC3-4230-BC40-E62AC276FF03}  Acomx Class
    {668456A8-24D6-4243-B106-B8F53F944640}  PSFactoryBuffer
    {67228205-C4C6-45D6-AAAE-CBF72A35D1B3}  PSFactoryBuffer
    {6AAF1B76-370B-427E-9D45-729A56826BD3}  PIN Class
    {729F85AE-A18C-42F4-8FF1-2861E829866D}  SmartCardConnectionManager Class
    {876DD103-9F92-4960-A705-4EC69B8B0ADA}  CardCriteria Class
    {8EB55F9F-C5DE-4727-BF28-7EA42AADE077}  PKCSInterface Class
    {9359DF4E-50D2-419E-989F-FF113D304593}  SKIAccessor Class
    {C0879BC8-FE3C-49CB-9D6F-3295F514E12A}  PINLogicalCriteria Class
    {CF323C11-8F18-4500-8301-0F99CCC2D054}  CSPInterface Class
    {D147D7C6-41F8-45E5-96C5-216657A9C173}  PSFactoryBuffer
Wed Dec 30 08:45:58 2015 Z
    {FAEA5B46-761B-400E-B53E-E805A97A543E}  Microsoft Office Visio Persistent Handler
Wed Dec 30 07:43:52 2015 Z
    {1BE75CA5-140F-4FBC-9A99-B522F1A1A30A}  RdpEndpoint Class
    {336000AA-AA9A-4988-B1D7-15F64E25182E}  PSFactoryBuffer
    {348ef17d-6c81-4982-92b4-ee188a43867a}  PrintDocumentPackageTargetFactory
    {5D52C3ED-4D79-4069-82B7-FBD600FC64B7}  PSFactoryBuffer
    {812F944A-C5C8-4CD9-B0A6-B3DA802F228D}  UIAnimationTransitionLibrary2
    {84302F97-7F7B-4040-B190-72AC9D18E420}  UIAnimationTransitionFactory2
```

Page 20

SOFTWARE OUTPUT.txt

```
{A7256C32-F6C3-4673-82BA-30764F9004DA}  RdpEndpoint Class
{A7C06739-500F-4E8C-99A8-2BD6955899EB}  PSFactoryBuffer
{C1A6713B-F5BA-4340-BFE5-07DA0ED49A27}  Superseded Updates Cleanup
{D25D8842-8884-4A4A-B321-091314379BDD}  UIAnimationManager2
{E1553E07-5939-4CFD-BE24-3BCEBA2F148C}  Proxy CLSID
{F02602C4-3C2A-473B-B35E-679A0076A4A5}  WatAdminSvcObject Class
{F1CA3CE9-57E0-4862-B35F-C55328F05F1C}  Windows Activation Technologies ActiveX
Control
{f4ba59cc-2506-45ae-84c8-78ea8d7f9b3e}  Compat Inventory WMI provider
Wed Dec 30 07:43:51 2015 Z
{0BE9F729-A4E0-4BED-9FB3-85F1858143B7}  SSPWorkspace Class
{301B94BA-5D25-4A12-BFFE-3B6E7A616585}  Microsoft RDP Client Control
(redistributable) - version 10
{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}
{33F3C8F8-27A1-4DF3-A525-E89CB18881A5}  Workspace Setup Discovery Page
{5F681803-2900-4C43-A1CC-CF405404A676}  Microsoft RDP Client Control
(redistributable) - version 9
{6B7F33AC-D91D-4563-BF36-0ACCB24E66FB}  MsRdpSessionManagerSingleUse Class
{7b40792d-05ff-44c4-9058-f440c71f17d4}  Windows trace relogging support.
{8B918B82-7985-4C24-89DF-C33AD2BBFBCD}  Microsoft RDP Client Control - version 10
{A3BC03A0-041D-42E3-AD22-882B7865C9C5}  Microsoft RDP Client Control - version 9
{E018945B-AA86-4008-9BD4-6777A1E40C11}
Wed Dec 30 07:41:07 2015 Z
{BE5018C3-A638-40C1-B4DA-1BE1448353B8}
{F2C4CDB0-2714-42AD-A948-2ED958A322E3}  WorkspaceResTypeRegistry Class
Tue Dec 29 18:43:07 2015 Z
{0CA545C6-37AD-4A6C-BF92-9F7610067EF5}  HNetCfg.FwOpenPort
{1fb2a002-4c6c-4de7-85c2-cb8db9a4f728}  Microsoft Disk Quota UI Elevation Helper
{26D32566-760A-40A2-AA82-A40366528916}  WUPublishedAppInstallorElevator Class
{2C5BC43E-3369-4C33-AB0C-BE9469677AF4}  HNetCfg.FwRule
{304CE942-6E39-40D8-943A-B913C40C9CD4}  HNetCfg.FwMgr
{4026492F-2F69-46B8-B9BF-5654FC07E423}  Windows Firewall
{78CB147A-98EA-4AA6-B0DF-C8681F69341C}  CardSpace
{E2B3C97F-6AE1-41AC-817A-F6F92166D7DD}  HNetCfg.FwPolicy2
{EC9846B3-2762-4A6B-A214-6ACB603462D2}  HNetCfg.FwAuthorizedApplication
Tue Dec 29 16:08:14 2015 Z
{DF912424-425A-4F52-985D-1F83DA468AEB}  MeetingJoinHelper Class
Tue Dec 29 16:07:32 2015 Z
{2C8810FD-43CD-460D-8FDF-E3A958175E9F}  TestUCInterface Class
{2CD5239C-7739-42F1-9C94-2A8E24A9BBD9}  OcForms Class
{444204E4-E468-4E97-8661-02D16A969A8C}  Profile Class
{5A0C06AC-5B0F-43A5-9E53-66F4CFAC7CC2}  Session Class
{5F45E1B6-90B2-43B5-BDF1-6DB4B4B0E35E}  TestUCMeeting Class
{6259C760-12AE-11D3-98AF-00C04F8D1CDE}  UCAddin Class
{756C4BDF-E406-4E9C-B18A-9FB142796748}  IUCAddinCallbackInterface Class
{7759C760-12AE-11D3-98AF-00C04F8D1CDE}  CollabAddin Class
{79A9A94F-4BA0-4D6C-B512-842F96ED1682}  MapiApplication Class
{843CEDFF-6D1B-40BA-AE3C-C32301A1623D}  FormRegionContext Class
{845263B8-8FC2-49CD-AE10-6781ABBC12A9}  OneNoteHelper Class
{856C4BDF-E406-4E9C-B18A-9FB142796748}  ICollabAddinCallbackInterface Class
{C43FB02F-FD2C-4F03-99E0-EBE681143C80}  Folder Class
{F1931D8E-51D3-496F-BE8A-3D08AEE9C9DB}  MS ATC Screen Decoder 1
Tue Dec 29 15:55:13 2015 Z
{0039FFEC-A022-4232-8274-6B34787BFC27}  Application Class
{D7FAC39E-7FF1-49AA-98CF-A1DDD316337E}  Application Class
Tue Dec 29 15:52:10 2015 Z
{138508bc-1e03-49ea-9c8f-ea9e1d05d65d}  @C:\Program Files\Microsoft
Office\Office14\MAPISHELL.DLL,-110
{1F2FD001-0148-474e-843E-D6D37A848D62}  Microsoft OneNote Windows Desktop Search
IFilter Base Class ID
{34CEAC8D-CBC0-4f77-B7B1-8A60CB6DA0F7}  Open Document Format ODT Persistent
Handler
{3B224B11-9363-407e-850F-C9E1FFACD8FB}  Zip Persistent Handler
```

Page 21

SOFTWARE OUTPUT.txt

```
{3DDEB7A4-8ABF-4D82-B9EE-E1F4552E95BE}   Open Document Format ODS Persistent
Handler
   {435fdba0-964c-43a7-8aff-cc94e21b2249}   Outlook MAPI Mail Previewer
   {4887767F-7ADC-4983-B576-88FB643D6F79}   Office Open XML Format Excel Persistent
Handler
   {4F46F75F-199F-4C63-8B7D-86D48FE7970C}   Office Open XML Format PowerPoint
Persistent Handler
   {942f72e2-b5ce-4e6c-8d76-0519b3f1bff7}   PSFactoryBuffer
   {B4132098-7A03-423D-9463-163CB07C151F}   Office Open XML Format Excel Persistent
Handler
   {D3B41FA1-01E3-49AF-AA25-1D0D824275AE}   Office Open XML Format Word Persistent
Handler
   {E2F83EED-62DE-4A9F-9CD0-A1D40DCD13B6}   Open Document Format ODP Persistent
Handler
   {e565b713-6e44-4c9d-8d01-ede208f88879}   Outlook Out Of Proc Mapi Handler
   {f64b4d4f-5196-4be6-ba86-ab6969c7608f}   PSFactoryBuffer
   {FB10BD80-A331-4e9e-9EB7-00279903AD99}   Office Outlook MSG Persistent Handler
Tue Dec 29 15:52:09 2015 Z
   {00020800-0000-0000-C000-000000000046}
   {00020812-0000-0000-C000-000000000046}
   {00020818-0000-0000-C000-000000000046}
   {00020819-0000-0000-C000-000000000046}
   {00020820-0000-0000-C000-000000000046}
   {00020821-0000-0000-C000-000000000046}
   {00024500-0000-0000-C000-000000000046}
   {0006F023-0000-0000-C000-000000000046}
   {0006F024-0000-0000-C000-000000000046}
   {0006F03A-0000-0000-C000-000000000046}
   {0006F04A-0000-0000-C000-000000000046}
   {0006F04B-0000-0000-C000-000000000046}
   {0006F04C-0000-0000-C000-000000000046}
   {0006F04D-0000-0000-C000-000000000046}
   {0006F04E-0000-0000-C000-000000000046}
   {0006F04F-0000-0000-C000-000000000046}
   {0006F050-0000-0000-C000-000000000046}
   {0006F051-0000-0000-C000-000000000046}
   {0006F053-0000-0000-C000-000000000046}
   {0006F054-0000-0000-C000-000000000046}
   {0006F055-0000-0000-C000-000000000046}
   {0006F056-0000-0000-C000-000000000046}
   {0006F057-0000-0000-C000-000000000046}
   {0006F058-0000-0000-C000-000000000046}
   {0006F059-0000-0000-C000-000000000046}
   {0006F063-0000-0000-C000-000000000046}
   {0006F067-0000-0000-C000-000000000046}
   {0006F068-0000-0000-C000-000000000046}
   {0006F069-0000-0000-C000-000000000046}
   {0468C085-CA5B-11D0-AF08-00609797F0E0}
   {1C3B4210-F441-11CE-B9EA-00AA006B1A69}
   {261B8CA9-3BAF-4BD0-B0C2-BF04286785C6}
   {490D6966-005D-36A5-B7EF-521A24207E7E}
   {4C599241-6926-101B-9992-00000B65C6F9}
   {59191DA1-EA47-11CE-A51F-00AA0061507F}
   {5CEF5610-713D-11CE-80C9-00AA00611080}
   {82B02373-B5BC-11CF-810F-00A0C9030074}
   {82B02374-B5BC-11CF-810F-00A0C9030074}
   {82B02375-B5BC-11CF-810F-00A0C9030074}
   {8A683C92-BA84-11CF-8110-00A0C9030074}
   {8A683C93-BA84-11CF-8110-00A0C9030074}
   {909E0AE0-16DC-11CE-9E98-00AA00574A4F}
   {91493441-5A91-11CF-8700-00AA0060263B}
   {91493443-5A91-11CF-8700-00AA0060263B}
   {91493446-5A91-11CF-8700-00AA0060263B}
```

Page 22

```
                              SOFTWARE OUTPUT.txt
     {91493448-5A91-11CF-8700-00AA0060263B}
     {AFC20920-DA4E-11CE-B943-00AA006887B4}
Tue Dec 29 15:52:08 2015 Z
     {00020906-0000-0000-C000-000000000046}
     {000209F0-0000-0000-C000-000000000046}
     {000209F1-0000-0000-C000-000000000046}
     {000209F2-0000-0000-C000-000000000046}
     {000209F4-0000-0000-C000-000000000046}
     {000209F5-0000-0000-C000-000000000046}
     {000209FF-0000-0000-C000-000000000046}
     {0002E101-0000-0000-C000-000000000046}
     {0002E119-0000-0000-C000-000000000046}
     {0002E132-0000-0000-C000-000000000046}
     {0002E169-0000-0000-C000-000000000046}
     {0002E170-0000-0000-C000-000000000046}
     {0002E174-0000-0000-C000-000000000046}
     {0002E178-0000-0000-C000-000000000046}
     {0002E17C-0000-0000-C000-000000000046}
     {0002E185-0000-0000-C000-000000000046}
     {0002E187-0000-0000-C000-000000000046}
     {0002E18B-0000-0000-C000-000000000046}
     {0006F045-0000-0000-C000-000000000046}
     {000CDB0D-0000-0000-C000-000000000046}
     {02F92C80-8F8E-101B-AF4E-00AA003F0F07}
     {044E54C5-B19B-11CE-A689-00AA003F0F07}
     {08F6C811-3CFD-11D1-98BC-006008197D41}
     {08F6C813-3CFD-11D1-98BC-006008197D41}
     {08F6C814-3CFD-11D1-98BC-006008197D41}
     {08F6C815-3CFD-11D1-98BC-006008197D41}
     {08F6C816-3CFD-11D1-98BC-006008197D41}
     {08F6C818-3CFD-11D1-98BC-006008197D41}
     {08F6C819-3CFD-11D1-98BC-006008197D41}
     {08F6C81A-3CFD-11D1-98BC-006008197D41}
     {08F6C81B-3CFD-11D1-98BC-006008197D41}
     {08F6C81C-3CFD-11D1-98BC-006008197D41}
     {08F6C81E-3CFD-11D1-98BC-006008197D41}
     {08F6C820-3CFD-11D1-98BC-006008197D41}
     {08F6C821-3CFD-11D1-98BC-006008197D41}
     {08F6C822-3CFD-11D1-98BC-006008197D41}
     {0D944D89-82BC-43DE-9659-699DD3FBCD72}
     {12DCE806-EA8A-46AA-88DF-C4486EDB78E3}
     {1C4367A8-EAEE-4C23-9582-4A229DF2403E}
     {20E823C2-62F3-4638-96BD-90F4F6784EBC}   zip Filter
     {27B378D1-DAE2-48a5-BB40-A1C2BA02631D}
     {27CE30A0-91FF-101B-AF4E-00AA003F0F07}
     {300471E0-7426-11CE-AB63-00AA0042B7CE}
     {312AB530-ECC9-496E-AE0E-C9E6C5392499}   office Open XML Format Excel Filter
     {32CDF9E0-1602-11CE-BFDC-08002B2B8CDA}
     {34bb52b0-e577-4285-a0ac-1a9b0eabfefd}   MAPI Shell Context Menu
     {367E582C-F71C-4BF9-AA1B-9F62B793E9C5}
     {3B06E945-E47C-11CD-8701-00AA003F0F07}
     {3B06E947-E47C-11CD-8701-00AA003F0F07}
     {3B06E949-E47C-11CD-8701-00AA003F0F07}
     {3B06E94B-E47C-11CD-8701-00AA003F0F07}
     {3B06E94D-E47C-11CD-8701-00AA003F0F07}
     {3B06E94F-E47C-11CD-8701-00AA003F0F07}
     {3B06E951-E47C-11CD-8701-00AA003F0F07}
     {3B06E953-E47C-11CD-8701-00AA003F0F07}
     {3B06E955-E47C-11CD-8701-00AA003F0F07}
     {3B06E957-E47C-11CD-8701-00AA003F0F07}
     {3B06E959-E47C-11CD-8701-00AA003F0F07}
     {3B06E95B-E47C-11CD-8701-00AA003F0F07}
     {3B06E95D-E47C-11CD-8701-00AA003F0F07}
                              Page 23
```

SOFTWARE OUTPUT.txt

```
{3B06E95F-E47C-11CD-8701-00AA003F0F07}
{3B06E961-E47C-11CD-8701-00AA003F0F07}
{3B06E963-E47C-11CD-8701-00AA003F0F07}
{3B06E965-E47C-11CD-8701-00AA003F0F07}
{3B06E967-E47C-11CD-8701-00AA003F0F07}
{3B06E970-E47C-11CD-8701-00AA003F0F07}
{3B06E973-E47C-11CD-8701-00AA003F0F07}
{3B06E979-E47C-11CD-8701-00AA003F0F07}
{3B06E986-E47C-11CD-8701-00AA003F0F07}
{3B06E989-E47C-11CD-8701-00AA003F0F07}
{3B06E993-E47C-11CD-8701-00AA003F0F07}
{3CA78EDC-E48A-4A21-9562-9245BF90CE3F}    Enterprise Projects
{3F1B1773-65CB-4DB9-9FC6-ACED47DB285A}
{4039B326-9F27-4B4A-B460-47A0C6A39D5C}    Office Outlook MSG IFilter
{416ED4F1-AB31-11D1-BF72-0060083E43CF}
{416ED4F7-AB31-11D1-BF72-0060083E43CF}
{4215CC2C-15B5-47A5-9B60-119BD269CB7E}
{4375351E-7052-40DF-B4D3-6095E7F8811B}
{4693FF15-B962-420A-9E5D-176F7D4B8321}    Open Document Format ODP Filter
{483615A0-74BE-101B-AF4E-00AA003F0F07}
{483615A0-74BE-101B-AF4E-00AA003F0F08}
{48E73304-E1D6-4330-914C-F5F514E3486C}    Send to OneNote from Internet Explorer
button
{493D8A73-1DB1-11D1-98A2-006008197D41}
{506F4668-F13E-4AA1-BB04-B43203AB3CC0}    ImageExtractorShellExt Class
{50D56610-60AC-11CF-82C9-00AA004B9FE6}
{5554F805-47C0-489D-AAE6-2D11C6E4A3ED}    OneNote NoteLinkStoreService Class
{5A98B233-3C59-4B31-944C-0E560D85E6C3}    Office Open XML Format Word Filter
{6D40D9DE-2821-44A8-BAF3-8011E362CF59}
{6E03AD86-431E-4879-A572-EF0EBA2FA729}
{6F3DD387-5AF2-492B-BDE2-30FF2F451241}
{73507951-A405-4E95-A197-B5FE6C6C001D}    OneNote NoteAnchor Class
{73778F0A-9743-4DF3-BBFA-941712488FEA}
{7398AAFD-6527-48C7-95B7-BEABACD1CA3F}
{73A4C9C1-D68D-11D0-98BF-00A0C90DC8D9}
{7AD9E906-BAF8-11CE-A68A-00AA003F0F07}
{7CCA70DB-DE7A-4FB7-9B2B-52E2335A3B5A}    Enterprise Projects
{805B7F91-C9CF-4EDF-ACA6-775664FDFB3E}
{8357BB51-95A2-4043-A040-2825FACEF50D}
{8357BB53-95A2-4043-A040-2825FACEF50D}
{8B06E321-B23C-11CF-89A8-00A0C9054129}
{8D4F994C-EBBE-4F8D-BA4B-AE20CD36E72D}
{8DE0A0A1-96D0-4B04-8EC6-2DBF9BD888DC}    QuickViewShellExt Class
{90B322A4-F1D9-11CD-8701-00AA003F0F07}
{9212BA72-3E79-11D1-98BD-006008197D41}
{95F35795-64B1-495D-9DE7-390EECC31EC0}    Microsoft Office Project Task Launch
Control
{977D8304-FAAA-4331-81DB-B67FC2134A38}    OneNote NoteLinkContentService Class
{97A2762C-403C-4953-A121-7A75ABCE4373}
{9CD4A762-A6A9-11CE-A686-00AA003F0F07}
{9E390D9E-7641-4819-BF38-8EEE08964681}    Office SPP WMI Provider
{9FBC2D8F-6F52-4CFA-A86F-096F3E9EB4B2}    Open Document Format ODT Filter
{A1EB89D6-0A9C-4575-A0AE-654A990A454C}
{A394DCA9-3727-11D4-BD85-00C04F6B93A4}    CVisioFileFilter Class
{AA533187-6399-4E6C-B6EC-6FC999E1C855}
{B06693E3-385D-4E70-923E-4FAB6D14EE15}
{BC9E4355-F037-11CD-8701-00AA003F0F07}
{BC9E4356-F037-11CD-8701-00AA003F0F07}
{BC9E4359-F037-11CD-8701-00AA003F0F07}
{BC9E435A-F037-11CD-8701-00AA003F0F07}
{BC9E435C-F037-11CD-8701-00AA003F0F07}
{BC9E435E-F037-11CD-8701-00AA003F0F07}
{BC9E4360-F037-11CD-8701-00AA003F0F07}
```

Page 24

SOFTWARE OUTPUT.txt

```
{BE39F3D6-1B13-11D0-887F-00A0C90F2744}
{BE39F3D7-1B13-11D0-887F-00A0C90F2744}
{BE39F3D8-1B13-11D0-887F-00A0C90F2744}
{BE39F3DA-1B13-11D0-887F-00A0C90F2744}
{CB9D3172-4728-11D1-8334-006008197CC8}
{CD7791B9-43FD-42C5-AE42-8DD2811F0419}
{D0B22D03-D05D-4C6D-8AB7-9392E84A87B9}
{D303AC37-74DB-45b9-8C22-AD7C3FBA68EF}
{D5EC4D34-77DA-4F7A-B8C4-8A910C1C1CFE}
{D66DC78C-4F61-447F-942B-3FB6980118CF}   CInfoTipShellExt Class
{D9160E22-BDF3-4D8A-818C-D99D10EC7BEF}   OSppWmiTokenActivationSigner
{D9230E09-3737-43F5-8C78-BC4C83DC296C}   OneNote NoteLinkMeta Class
{DA936B63-AC8B-11D1-B6E5-00A0C90F2744}
{DBC5175E-A8ED-11D3-A0DD-00C04F68712B}
{DBC51761-A8ED-11D3-A0DD-00C04F68712B}
{DDFE337F-4987-4EC8-BDE3-133FA63D5D85}   Office Open XML Format PowerPoint Filter
{E27A992D-A330-11D0-81DD-00C04FC2F51B}
{E2F5480E-ED5A-4DDE-B8A8-F9F297479F62}   Open Document Format ODS Filter
{E87ECCF7-3CBA-45CF-B58E-1A6630D39199}   OneNote NoteAnchorCollection Class
{EB106214-9C89-11CF-A2B3-00A0C90542FF}
{ECD1EADA-D373-11D3-8D21-0050048383FB}
{EF1A0B1D-AD6D-48E6-9905-BEE2A5D38DF9}
{F5BF6FE9-913F-4117-94C7-5040C7E3A6C1}   IconHandlerShellExt Class
{F8C9DCB3-4063-490E-A73C-3533207CBC26}
{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}   Office Open XML Format Excel Filter
{FF240263-AF0A-432D-A544-A721E75738F8}
{FFFDC614-B694-4AE6-AB38-5D6374584B52}   Linked Notes button
Tue Dec 29 15:52:07 2015 Z
{02BCC737-B171-4746-94C9-0D8A0B2C0089}   Microsoft Office Template and Media
Control
{0875DCB6-C686-4243-9432-ADCCF0B9F2D7}   Microsoft OneNote Namespace Extension for
Windows Desktop Search
{0BA70019-98B1-4B44-9DC5-9AF8634B1C25}   Groove Icon Overlay Loader
{1668B852-A887-4C5F-888A-7D666FBB283A}   Microsoft SharePoint Workspace Embedded
File
{16F3DD56-1AF5-4347-846D-7C10C4192619}   Groove Explorer Icon Overlay 3 (GFS
Folder)
{274C2936-A842-45f3-A457-FB4BA4ED1BA2}   VSTO Controller
{2916C86E-86A6-43FE-8112-43ABE6BF8DCC}   Groove Explorer Icon Overlay 4 (GFS Unread
Mark)
{2A541AE1-5BF6-4665-A8A3-CFA9672E4291}   Groove Folder Synchronization
{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}   VSTO SmartTag Recognizer
{387E725D-DC16-4D76-B310-2C93ED4752A0}   Groove XML Icon Handler
{3D60EDA7-9AB4-4DA8-864C-D9B5F2E7281D}   Workspaces
{42042206-2D85-11D3-8CFF-005004838597}
{421F717F-692A-4F50-AE1F-AFF4140C45BF}   Microsoft SharePoint Workspace Embedded
Ink
{4E3C66D5-58D4-491E-A7D4-64AF99AF6E8B}   VSTO Loader
{4FCEE402-10E9-4446-AE0F-AE48D6D62E9A}   Groove Site Client ActiveX
{64654B35-A024-4807-89D3-C6FDB5A260C7}   VSTO FormRegionsHostX
{6550EDEF-141E-4048-92BE-3C641C474013}   Local Groove Web Services Provider
{6C467336-8281-4E60-8204-430CED96822D}   Groove GFS Context Menu Handler
{6EE84065-8BA3-4a8a-9542-6EC8B56A3378}   Microsoft OneNote Windows Desktop Search
IFilter
{72773E1A-B711-4d8d-81FA-B9A43B0650DD}   Microsoft OneNote Windows Desktop Search
IFilter Persistent handler
{72853161-30C5-4D22-B7F9-0BBC1D38A37E}   Groove GFS Browser Helper
{760681E7-B985-41CE-BCBE-2985A1DFC61C}   VSTO Assembly100
{807573E5-5146-11D5-A672-00B0D022E945}   Microsoft Office InfoPath XML Mime Filter
{83081C08-382C-4ED4-ACCF-DCBECA021010}   VSTO Accessor class
{920E6DB1-9907-4370-B3A0-BAFC03D81399}   Groove Explorer Icon Overlay 2.5 (GFS
Unread Folder)
{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}   Microsoft Office Metadata Handler
```

Page 25

```
                        SOFTWARE OUTPUT.txt
    {99D651D7-5F7C-470E-8A3B-774D5D9536AC}  VSTOAddinLoader
    {99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}  VSTO SmartTag Action
    {99FD978C-D287-4F50-827F-B2C658EDA8E7}  Groove Explorer Icon Overlay 1 (GFS Unread
Stub)
    {A249E9F6-5B28-4ED1-8AF0-C9B9C5195486}  PaneLocator Class
    {A37BBB42-E8C1-4E09-B9CA-F009CE620C08}  VSTO WinFormsHost Control
    {A449600E-1DC6-4232-B948-9BD794D62056}  Groove GFS Stub Icon Handler
    {AB5C5600-7E6E-4B06-9197-9ECEF74D31CC}  Groove Explorer Icon Overlay 2 (GFS Stub)
    {AB968F1E-E20B-403A-9EB8-72EB0EB6797E}
    {B0FBD52D-C4A7-4A19-985D-11309D1AC8AE}  SharePoint Workspace Search Protocol
Handler
    {B4F3A835-0E21-4959-BA22-42B3008E02FF}  Office Document Cache Handler
    {B5A7F190-DDA6-4420-B3BA-52453494E6CD}  Groove GFS Stub Execution Hook
    {B5C71A93-FA82-4672-8B6A-E2C0FF64FF9D}  Groove Application
    {B7EFF951-E52F-45CC-9EF7-57124F2177CC}  SmartDocument Class
    {B8D12492-CE0F-40AD-83EA-099A03D493F1}  Microsoft OneNote Filter
    {C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97}  Microsoft Office Thumbnail Handler
    {C514A18E-862A-45d3-8A5E-62CF54D912B6}  Microsoft Office 14 Authorization Control
    {C7DFFDF1-BD1F-450A-B98D-96B6D30BA4C1}  Microsoft OneNote Windows Desktop Search
Protocol Handler
    {CB3F7806-3CB4-409C-BA3B-12D642BE371A}  Launcher
    {E46D1FAF-5B42-40C7-88B9-C702A6E9FE74}  Groove Dummy Shell Extension
    {E772CEB3-E203-4828-ADF1-765713D981B8}  Microsoft OneNote Section persistent
handler
    {E886F1D9-7842-485D-8EDF-9E1C7062A483}  Groove OutlookProxyAddIn
    {EC04D82C-AA59-4ba4-96B1-27BE3FF05E00}  VSTO Mime Handler
    {F09D237B-3FD1-4900-BEF2-3471CA68142D}  VSTO CTPHostX
Tue Apr 12 07:45:35 2011 Z
    {0eb06e8d-d00a-11da-a46c-0040f4b33241}  TSErrRedir
    {565E978D-AC10-443A-A2C8-165C2DA1B5FC}  Sticky Notes Windows Desktop Search
Protocol Handler
    {F3F5824C-AD58-4728-AF59-A1EBE3392799}  Sticky Notes Namespace Extension for
Windows Desktop Search
Tue Apr 12 07:45:34 2011 Z
    {00C6D95F-329C-409a-81D7-C46C66EA7F33}  DefaultLocation
    {010911E2-F61C-479B-B08C-43E6D1299EFE}
    {0245858B-948D-4f36-A574-1A71EF5111CB}
    {0365BE92-BD3F-47f5-8BB6-2EEF7AF5CAE7}  SimpleInputItem Class
    {054AAE20-4BEA-4347-8A35-64A533254A9D}  UIHost Class
    {06DA0625-9701-43da-BFD7-FBEEA2180A1E}  HotStart User Agent
    {075DB5A6-4C67-4816-AE00-7451EC2AAA51}  NBDocument Class
    {07DC68FA-A15D-4E44-93DE-645060C7B469}  HandWritingSkinProps Class
    {09F81337-D568-41d1-A177-D6779AF55847}  WBEM WIN32_TSVIRTUALIPSETTING Provider
    {0AEA3667-1039-43ff-8D21-B1A162090671}  AppIdPolicyHelper Class
    {0FDE5092-AA2A-11D1-A7D4-0000F87571E3}  Group Policy About Information
    {10CFC467-4392-11d2-8DB4-00C04FA31A66}  Offline Files Folder Options
    {14834D34-8CEE-459e-8520-2264EC46E099}  SharedHWProperties Class
    {15D633E2-AD00-465b-9EC7-F56B7CDF8E27}  Tablet PC Input Panel
    {19371BCB-2BFF-4F74-BB8E-3ABEA71B9E7D}  InkWatsonWizard
    {1BC972D6-555C-4FF7-BE2C-C584021A0A6A}  Software installation
    {1E2D67D6-F596-4640-84F6-CE09D630E983}  ShapeCollector Class
    {1FF28512-6C1F-4CC2-BB1D-948DD60DB711}
    {2331D136-E39D-4019-92D6-7CE5579962FB}  Sensors Sensor Configuration Helper
    {23571E11-E545-4DD8-A337-B89BF44B10DF}  PSFactoryBuffer
    {289AE5EE-562C-4350-A8CB-0CB0587A12FF}
    {28F4700C-44EB-4BD8-BC25-95812DE98E08}  PPCNode Class
    {2DCD1DAF-A110-49c0-BFDB-6FDF557B5FDF}  Offline Files WMI Provider
    {2E1AE5DF-5A6F-420A-9B7B-41E5BA8FA36D}  HWProp Class
    {2E483DC9-7E4D-4861-B496-7E00B7FA184F}  NbTextLayoutPageText Class
    {2F248FAD-47C5-42a8-9672-61095D712258}
    {3429E395-176B-4a0a-863D-FCA6B19073BA}  GeneralProperties Class
    {357b663c-d9fa-4188-99af-2943920f96c5}  PSFactoryBuffer
    {3697C5FA-60DD-4B56-92D4-74A569205C16}  Tablet PC Correction for Windows Journal
```

Page 26

SOFTWARE OUTPUT.txt

```
{39524FB7-028F-4035-8C2B-8E65D2B17E67}  WBEM WIN32_TSSESSIONDIRECTORY Provider
{39C42C60-85F5-40ED-BF39-975A0AA0B2A4}  HandWritingSkin Class
{3B68879A-2CE5-419D-BB70-F39E1F66B06F}  MathRecognizer Class
{3F13AB10-AE95-48AA-8C94-533730760A20}  PMCRootNode Class
{40B6664F-4972-11D1-A7CA-0000F87571E3}  Scripts (Startup/Shutdown)
{40B66650-4972-11D1-A7CA-0000F87571E3}  Scripts (Logon/Logoff)
{40B66660-4972-11D1-A7CA-0000F87571E3}  Scripts (Startup/Shutdown)
{40B66661-4972-11D1-A7CA-0000F87571E3}  Scripts (Logon/Logoff)
{42D69529-136E-49D6-8407-3026853038BF}  PMCComponent Class
{450D8FBA-AD25-11D0-98A8-0800361B1103}
{45F26E9E-6199-477F-85DA-AF1EDFE067B1}  SessionAgent Class
{46445657-1F22-11DA-A2D9-00065B83EE53}  PSFactoryBuffer
{474C98EE-CF3D-41f5-80E3-4AAB0AB04301}
{48C6BE7C-3871-43cc-B46F-1449A1BB2FF3}  Offline Files Cache Control
{494C063B-1024-4DD1-89D3-713784E82044}  CoBrmEngine Class
{4B0A2997-E555-4F84-B45B-68AB8BC57635}  RdpEndpoint Class
{4C8A0917-F587-4ECF-9C89-48147528F4E1}  WBEM WIN32_TSGENERALSETTING Provider
{4CE576FA-83DC-4f88-951C-9D0782B4E376}  UIHostNoLaunch Class
{4E77131D-3629-431c-9818-C5679DC83E81}
{4EA9D6EF-694B-4218-8816-CCDA8DA74BBA}  SensorDataReport Class
{4F637904-2CAB-4F0E-8688-D3717EBD2975}  Group Policy About Information
{4FDDEA74-513D-4454-90B4-4AB1011157AD}  Stationery Class
{4FE8C25F-C8E9-4322-98EE-A11E117CF049}  MachineComponentData Class
{50422459-63B3-4e9f-93C7-7B068517C027}
{50A7B286-7D23-41E6-9440-4DAEE00DC5F0}  LogicalSensorManager Class
{56C4F5A2-E217-4610-83CC-89F09E07782B}  NbCompositeLayer Class
{5828227c-20cf-4408-b73f-73ab70b8849f}  UMRDPProtocolManager  Class
{5971EC44-072A-41b7-8E67-D9E045CC196D}  AppIdMmcPolicyHandler Class
{59B7D16A-C309-47C4-9667-363B9B8D8255}  PSFactoryBuffer
{5d8539fa-9e3b-459f-8118-020b5ef1796e}  JNT Persistent Handler
{5ea4f148-308c-46d7-98a9-49041b1dd468}  Mobility Center Control Panel
{5ED98377-87A3-4d86-81F7-3E46E0342833}  AdvancedProperties Class
{6101F767-998E-452B-B54A-E836DD486BAD}  SensorClassExtension Class
{63E23168-BFF7-4E87-A246-EF024425E4EC}  RSOP Context Menu
{643B0017-1AAE-4AFA-B921-4BE3FB8308A2}  WMI Provider for Terminal Services
Publishing
{64445657-9101-11d9-994B-00301BB132BA}  InkItem Class
{647BD8C2-658B-4ECA-ABC7-FC5C0BF1704D}  WBEM WIN32_TSCLIENTSETTING Provider
{673F14E0-1875-42a1-90F9-647F4AD9DB92}
{68E1DF8C-9512-4801-A105-25A44DCCB164}
{69486DD6-C19F-42e8-B508-A53F9F8E67B8}  Offline Files Service Control
{69D76D1B-B12E-4913-8F48-671B90195A2B}  Microsoft WBEM WMI Policy Status Provider
{6B19643A-0CD7-4563-B710-BDC191FCAD3B}  TSFstateManager Class
{6B56A227-7150-4A1F-A114-C959EB8F8C24}  Software Installation Group Policy User
Profile Notification
{6BD6AECA-AFB0-45B7-BAC4-F292EC0F3F41}  WBEM Win32_TERMINALSERVICESETTING Provider
{6CE51F75-0448-438e-B9CA-69C352A248A7}  Sensors CPL Change Device Permission LUA
Helper
{6DC3804B-7212-458D-ADB0-9A07E2AE1FA2}  Resultant Set of Policy
{70445657-5AB0-11d9-A4E5-00301BB132BA}  InkStore Class
{71B804C5-5577-471D-8FE5-C4A45B654EB8}  Windows SideShow AutoWake Configuration
Helper
{7295965A-230A-4F34-AD5F-B15C9120F6E4}
{73EB8142-4A74-49FD-A0FC-05FAEED4CD51}  Advanced Audit Policy Group Policy Editor
Extension
{74628299-57EC-4F12-BA1C-08B477BF447A}  WBEM WIN32_TERMINAL Provider
{74ABD359-DD57-46b2-B459-B8FC803E67D4}  TipSettings Class
{750fdf10-2a26-11d1-a3ea-080036587f03}  Offline Files Synchronization Handler
{76052C5C-2EB4-4C40-B1F1-2A5C8554590A}  Connect to a Network Projector
{76AE5F57-B7C9-421f-B55E-FB25144317B6}  Sensors CPL Change Description LUA Helper
{76DC8129-0A40-45eb-B0DC-09E8C6CDDE9D}  NbTextLayoutPageProp Class
{76EFD608-E0CE-4887-98E2-F931363C4BC5}  SideShowClassExtension Class
{7757BA9B-7986-4866-B53F-A31E89FCBA15}  WBEM WIN32_TSNETWORKADAPTERLISTSETTING
```

Page 27

SOFTWARE OUTPUT.txt
```
Provider
    {77A1C827-FCD2-4689-8915-9D613CC5FA3E}    SensorManager Class
    {7970614A-BD82-439E-A828-CC96F8E91428}    WBEM WIN32_TERMINALSERVICE Provider
    {79C43ADB-A429-469F-AA39-2F2B74B75937}    SensorCollection Class
    {7C606A3F-8AA8-4E36-92D6-2B6AFEC0B732}    PMCPrintQueueViewExtension Class
    {7CCA6768-8373-4d28-8876-83E8B4E3A969}    SDPWmiJob Class
    {7E45546F-6D52-4D10-B702-9C2E67232E62}    Software installation
    {7EFA68C6-086B-43e1-A2D2-55A113531240}
    {802B1FB9-056B-4720-B0CC-80D23B71171E}    Microsoft PenInputPanel Control
    {807C1E6C-1D00-453f-B920-B61BB7CDD997}    Microsoft TipAutoCompleteClient Control
    {83FEFA40-6F67-4244-AA04-1E590C1CB1D9}    TextContributor Class
    {84DE202D-5D95-4764-9014-A46F994CE856}    Administrative Templates - Starter GPO
(Computer)
    {84DE202E-5D95-4764-9014-A46F994CE856}    Administrative Templates - Starter GPO
(User)
    {8613E14C-D0C0-4161-AC0F-1DD2563286BC}    Correction Widget Class
    {86950435-ED12-42ef-A807-061E5E7CA99F}
    {88EEBD3A-9091-44b8-92A7-F0D595422D90}    GesturesProperties Class
    {8A539A30-0653-4E54-91B8-C8CF5DE862A1}    RichInkSegment Class
    {8BA2F157-CC2D-4d7a-BE0B-99C53DB78F10}    NbDocCstg Class
    {8C24BE77-7E9E-4d5c-85F7-EFC393B5FEC4}    NbBaseEditableDocument Class
    {8FC0B734-A0E1-11D1-A7D3-0000F87571E3}    Local Group Policy Editor
    {901AB1E6-3EC9-4aae-AEE5-188013A5CC21}    RioEventSender Class
    {9209B7D1-6DA5-43E4-BCD1-F2BE497635E7}    RdpEndpoint Class
    {942A8E4F-A261-11D1-A760-00C04FB9603F}    Software installation
    {9859049F-C6D1-4e66-B0F8-188FF1064E3C}    CompositeInputItem Class
    {9A17DFD1-34FA-4D61-B9BB-3A1097E7FADF}    WBEM WIN32_TSENVIRONMENTSETTING Provider
    {9A630456-078D-43d3-9F1D-DF7A5BC0FA44}    Default Location CPL Data Handler LUA
Helper
    {9b359d1b-ad5c-412f-a654-a431424359de}    Offline Files Profile Notify Handler
    {9C4D3346-650D-472d-A867-6F595B39D973}    AuditPolicyGPHandler Class
    {9CE24FD4-94CB-4a9a-A19D-1B0F819005B7}
    {9F074EE2-E6E9-4d8a-A047-EB5B5C3C55DA}    HwTextInsertion Class
    {A0ADD4EC-5BD3-4f70-A47B-07797A45C635}
    {A666634D-333F-4CC9-AF78-65ED7DB1D6C3}    PSFactoryBuffer
    {a81d181b-0fd4-4442-91a1-b6febfaf1dc6}    Journal File Filter Class
    {AAEAE72F-0328-4763-8ECB-23422EDE2DB5}    Microsoft WBEM WMI Policy SOM Provider
    {AFDB1F70-2A4C-11d2-9039-00C04F8EEB3E}    Offline Files Folder
    {AFE0D06B-E242-47ea-A987-74EB2D1030E6}    NbTextLayoutPage Class
    {B03B16C7-35A7-4A55-BEF1-8876E1CE2F45}    PMCAbout Class
    {B29D466A-857D-35BA-8712-A758861BFEA1}
Microsoft.GroupPolicy.AdmTmplEditor.GPMAdmTmplEditorManager
    {B490264C-8D8F-40FD-B1BE-CD69AD779EC1}    WBEM WIN32_TERMINALSERVICETOSETTING
Provider
    {B6B44A97-B802-4d6e-9846-3AB9C0965C43}
    {B6F9C8AE-EF3A-41C8-A911-37370C331DD4}    Administrative Templates (Computers)
    {B6F9C8AF-EF3A-41C8-A911-37370C331DD4}    Administrative Templates (Users)
    {B7A44F26-0114-4285-B4BA-C9E78C4F9416}    NbDocView Class
    {BA4EAC04-AFCE-441A-A4F0-C4A97545425A}    WBEM WIN32_TERMINALTERMINALSETTING
Provider
    {BA9FCBAC-3AE4-46BF-B7BA-669498CCC8DE}    CPreferredTIPState Class
    {BACF5C8A-A3C7-11D1-A760-00C04FB9603F}    Software installation
    {BB5331F1-D8FF-4DDB-8A8F-2DF901123B33}    PPCRootNode Class
    {BDE24877-01D7-4103-9704-F0EC82FA7CE9}    UserComponent Class
    {BDF9E8B8-6C66-4E45-BA15-E050393DD079}    WBEM WIN32_TSACCOUNT Provider
    {BE9B3133-250B-44A5-A278-C532B7B7FF76}    WBEM WIN32_TSSESSIONSETTING Provider
    {BF0B4450-B1F8-4238-98B1-9CE4544D5673}
    {C41FF872-07B1-4926-819B-8C94E6B1FBB9}    WBEM WIN32_TSLOGONSETTING Provider
    {C4457F51-993A-4b98-A19B-EC2B4F0DA087}    AppLocker Configuration Tool
    {C4D6E899-E38A-4838-9188-0B98EE3175E6}    ProgrammabilityManager Class
    {C4D77430-755D-4E19-A6E1-AA8CA5E0E7BC}    TipTsfData Class
    {C51F0A6B-2A63-4cf4-8938-24404EAEF422}
    {C561816C-14D8-4090-830C-98D994B21C7B}    MathInputControl Class
```
Page 28

```
                         SOFTWARE  OUTPUT.txt
    {CB35832D-0C2C-41A9-84E1-A7CD1E0C6254}   UserComponentData Class
    {CB445657-116F-11D8-941D-00065B83EE53}   PSFactoryBuffer
    {CCBA37FC-982B-433B-8AC2-455E616A8559}   WBEM WIN32_TSSESSIONDIRECTORYSETTING
Provider
    {D02B1F72-3407-48ae-BA88-E8213C6761F1}   Administrative Templates (Computers)
    {D02B1F73-3407-48ae-BA88-E8213C6761F1}   Administrative Templates (Users)
    {D06342BD-9057-4673-B43A-0E9BBBE99F11}   PMCComponentData Class
    {D25E0260-AAB7-48CB-A192-4D73D2FD375F}   WBEM WIN32_TSNETWORKADAPTERSETTING
Provider
    {D3667F1E-CCB8-4A69-99DF-59A2B2A6753F}   Windows SideShow Device Configuration
Helper
    {D5C82393-AB49-47e9-BE80-B7801443BE43}
    {D6E88812-F325-4dc1-BBC7-23076618E58D}   TsfManager Class
    {D9EF8727-CAC2-4e60-809E-86F80A666C91}   Secure Startup
    {DB49BBEB-C744-49F8-81AC-AF97669D4CB0}   PrinterStatusHTMLViewExtension Class
    {DBD71B6B-F717-4A61-A914-2337BC50B0D6}   WBEM WIN32_TSREMOTECONTROLSETTING Provider
    {E25E57E9-DA9C-4A35-A0D8-CFB5EA6AF7E6}   Advanced Audit Policy Configuration
    {E4E54B1D-1AC1-405c-B62A-E11CD87F2261}
    {E51DFD48-AA36-4B45-BB52-E831F02E8316}   AutoWakeTaskHandler Class
    {E7F34D0A-582E-4a48-98BA-6E58AAA3AD4C}   Sensors PropertyPage Host
    {E94137E0-92ED-4579-9251-18AF2A08CCD1}   Tablet Tip Soft Keyboard Skin Class
    {E95A4861-D57A-4be1-AD0F-35267E261739}   Windows SideShow
    {E97CED00-523A-4133-BF6F-D3A2DAE7F6BA}   Sensor Class
    {E9950154-C418-419e-A90A-20C5287AE24B}   Sensors
    {EACFAA1F-A6CB-4d4a-83D9-810F84C11803}
    {EBDD6BF3-AF35-4bf1-9EE3-335A3F5DE0FF}   NbAccessibleObject Class
    {EC278F3A-BFE8-42d5-99C0-E25F5EF4A3D1}   WBEM WIN32_TSVIRTUALIP Provider
    {ED834ED6-4B5A-4bfe-8F11-A626DCB6A921}   Personalization Control Panel
    {EF6EF542-EB19-4986-89D3-143960609251}   MachineComponent Class
    {EFB23A09-A867-4BE8-83A6-86969A7D0856}   PSFactoryBuffer
    {F056D291-A2AB-45f7-8EE4-40454493B351}   Windows SideShow PropertyPage Host
    {F1ED7D4C-F863-4de6-A1CA-7253EFDEE1F3}   AppIdPolicyHandler Class
    {F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6}   CPenIMX Class
    {F3B4F2E9-CCCC-49aa-B0B2-2C4A02E69A37}   TabTipUI Class
    {F87CB264-80B7-4df8-9E62-ABC259074CF6}   NbRioEventSink Class
    {F9B189D7-228B-4F2B-8650-B97F59E02C8C}   Microsoft TextInputPanel Object
    {FA06375D-F0A4-4A47-AD8D-148595F1E0B8}   WBEM WIN32_TSPERMISSIONSSETTING Provider
    {FA3F3DD9-4C1A-456B-A8FA-C76EF3ED83B8}   Offline Files Background Synchronization
Task Handler
    {FC138128-D766-4f2a-9EA6-6C88E3EC2301}   NbBitmapLayer Class
    {FD3659E9-A920-4123-AD64-7FC76C7AACDF}   Offline Files Setting Object
    {FD76C304-255F-4446-A895-6E1967EC4FDC}   AppLocker Group Policy Editor Extension
    {FD8D7237-49E4-4B99-A580-ACA91ED6FCDA}   RioTabletInput Class
    {FF87090D-4A9A-4f47-879B-29A80C355D61}   GadgetsManager Class
Tue Apr 12 07:45:21 2011 Z
    {BFC006EE-B806-4C2A-A938-6D3344781512}
Sun Nov 21 03:40:13 2010 Z
    {0F0C09C5-601E-4396-BCD0-CDB343D7F657}   SSTP Configuration Configuration Notify
Object
    {6E65CBC0-926D-11D0-8E27-00C04FC99DCF}   Dial-Up Client Configuration Notify Object
    {6E65CBC1-926D-11D0-8E27-00C04FC99DCF}   Dial-Up Server Configuration Notify Object
    {6E65CBC3-926D-11D0-8E27-00C04FC99DCF}   NdisWan Configuration Notify Object
    {6E65CBC4-926D-11D0-8E27-00C04FC99DCF}   PPTP Configuration Configuration Notify
Object
    {6E65CBC5-926D-11D0-8E27-00C04FC99DCF}   Steelhead Router Configuration Notify
Object
    {6E65CBC6-926D-11D0-8E27-00C04FC99DCF}   L2TP Configuration Configuration Notify
Object
    {7177c4bd-e20a-4140-ad8a-998e7a2d18c0}   AGILEVPN Configuration Configuration
Notify Object
    {e949da38-c39d-4460-8ea7-a39152c56836}   PPPOE Configuration Configuration Notify
Object
Sun Nov 21 03:39:53 2010 Z
```

Page 29

SOFTWARE OUTPUT.txt
    {0C41D1E6-9D16-41ED-9CDD-D0665039857B}  Microsoft TCP/IP Version 6 Configuration
Notify Object
    {A907657F-6FDF-11D0-8EFB-00C04FD912B2}  Microsoft TCP/IP Configuration Notify
Object
Sun Nov 21 03:39:29 2010 Z
    {CD000001-8B95-11D1-82DB-00C04FB1625D}  CDOMessage Class
    {CD000002-8B95-11D1-82DB-00C04FB1625D}  CDOConfiguration Class
    {CD000004-8B95-11D1-82DB-00C04FB1625D}  CDO DropDirectory class
    {CD000005-8B95-11D1-82DB-00C04FB1625D}  SMTP OnArrival Script Host Sink Class
    {CD000006-8B95-11D1-82DB-00C04FB1625D}  NNTP OnPost Script Host Sink Class
    {CD000007-8B95-11D1-82DB-00C04FB1625D}  NNTP OnPostFinal Script Host Sink Class
    {CD000008-8B95-11D1-82DB-00C04FB1625D}  SMTPConnector Class
    {CD000009-8B95-11D1-82DB-00C04FB1625D}  NNTPPostConnector Class
    {CD000010-8B95-11D1-82DB-00C04FB1625D}  NNTPFinalConnector Class
    {CD000011-8B95-11D1-82DB-00C04FB1625D}  NNTPEarlyConnector Class
    {CD000012-8B95-11D1-82DB-00C04FB1625D}  NNTP OnPostEarly Script Host Sink Class
    {E3A9BD50-51AE-410f-9706-0BA0D68B9A94}  Scavenged Files Cleanup
Tue Jul 14 04:54:39 2009 Z
    {0F7434B6-59B6-4250-999E-D168D6AE4293}
    {1D6322AD-AA85-4EF5-A828-86D71067D145}  UIAnimationTransitionLibrary
    {2854F705-3548-414C-A113-93E27C808C85}  Enhanced Storage Context Menu Handler
Class
    {32665929-D77E-4ab5-8C08-FBF409B8A233}
    {32BA16FD-77D9-4AFB-9C9F-703E92AD4BFF}  CtTuner Class
    {36F54939-CD3B-4C73-92D5-F9A389ED631C}  Enhanced Storage Autoplay Handler Class
    {4C1FC63A-695C-47E8-A339-1A194BE3D0B8}  UIAnimationManager
    {641ABA69-56FD-4029-A445-4D8375D3A699}  UIAnimationDiagnostic
    {886D29DD-B506-466B-9FBF-B44FF383FB3F}  EnhancedStorageSiloAction Class
    {8A9B1CDD-FCD7-419c-8B44-42FD17DB1887}  UIAnimationTransitionFactory
    {9113A02D-00A3-46B9-BC5F-9C04DADDD5D7}  Enhanced Storage Data Source
    {926749fa-2615-4987-8845-c33e65f2b957}
    {af076a15-2ece-4ad4-bb21-29f040e176d8}  EnhancedStorageACT Class
    {BFCD4A0C-06B6-4384-B768-0DAA792C380E}  UIAnimationTimer
    {C608E099-892D-4628-B6A2-97257B014E2E}
    {cb25220c-76c7-4fee-842b-f3383cd022bc}  EnhancedStorageSilo Class
    {CC55EE92-FE67-43C9-95E7-E646918A4A04}  Enhanced Storage Command Handler
    {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}  Enhanced Storage Icon Overlay Handler
Class
    {f4d8c39a-f43d-42b4-9bdf-4e48d3044ba0}  Name Resolution Policy
    {fe841493-835c-4fa3-b6cc-b4b2d4719848}  EnumEnhancedStorageACT Class
Tue Jul 14 04:54:38 2009 Z
    {D212B88E-8365-4CA9-BC4E-CFA4251F6B5F}  NdisCap Notify Object
    {FCDC2CF5-ABCD-4BA5-94DA-1823AE06FE2B}  CorrelationEngine Class
Tue Jul 14 04:54:37 2009 Z
    {D17D1D6D-CC3F-4815-8FE3-607E7D5D10B3}  Text to Speech Control Panel
Tue Jul 14 04:54:36 2009 Z
    {ca767aa8-9157-4604-b64b-40747123d5f2}  RegistryIdleBackupHandler
Tue Jul 14 04:54:32 2009 Z
    {0003000A-0000-0000-C000-000000000046}  Bitmap Image
    {08229782-89C8-4028-BB74-75BB58EF1488}  IP Security Monitor
    {1fda955b-61ff-11da-978c-0008744faab7}  Detection And Sharing
    {1fda955c-61ff-11da-978c-0008744faab7}  PSFactoryBuffer
    {57C596D0-9370-40C0-BA0D-AB491B63255D}  IP Security Monitor
    {A17DA8D0-F67D-47A0-9EC4-19C486383206}  IP Security Monitor
    {A2A54893-AAF2-49A3-B3F5-CC43CEBCC27C}  Network Access Protection GPEdit Extension
    {ABB78EBD-45BD-415B-9466-5C2A0F25CACE}
    {B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC0}  @%systemroot%\system32\eqossnap.dll,-30001
    {B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC1}  @%systemroot%\system32\eqossnap.dll,-30001
    {C1060E7E-7939-44A5-99C3-A6DCCD92AED0}  , PSFactoryBuffer
    {D3E34B21-9D75-101A-8C3D-00AA001A1652}  Paintbrush Picture
    {DEA8AFA0-CC85-11D0-9CE2-0080C7221EBD}  Create and edit Internet Protocol Security
policies
    {DEA8AFA1-CC85-11D0-9CE2-0080C7221EBD}  Create and edit Internet Protocol Security
Page 30

SOFTWARE OUTPUT.txt

```
policies
    {DEA8AFA2-CC85-11D0-9CE2-0080C7221EBD}  Create and edit Internet Protocol Security
policies
    {ff258fc0-99b1-4297-b857-539ad9bc13ed}  Cert Enrollment Class
Tue Jul 14 04:54:31 2009 Z
    {06993B16-A5C7-47EB-B61C-B1CB7EE600AC}  Create and edit Wired policies
    {22BDC741-73F0-41DB-9463-E343DEF3E376}  PSFactoryBuffer
    {24FF4FDC-1D9F-4195-8C79-0DA39248FF48}  Quarantine Private SHA Binding class
    {2D4156A2-897A-11DB-BA21-001185AD2B89}  Network List Manager Snapin
    {2D4156A5-897A-11DB-BA21-001185AD2B89}  Network List Manager Snapin About
Interface
    {388D606F-AF7B-4AD2-AC22-6B4FE70CE286}  Create and edit Wired policies
    {38B22A43-49A8-45ab-BEB7-9137A488B1D3}  Quarantine Private QA Management class
    {44C39C96-0167-478F-B68D-783294A2545D}  Manage Network Names
    {677126ed-2a91-40ff-8c52-06181c064573}  NAP Elevated class
    {8E594310-16CA-4a00-932F-F70969F990C0}  Quarantine System Health Agent Binding
class
    {9443B89B-6564-496a-B19C-6C6D22709045}  Quarantine Enforcement Client Binding
class
    {9a010fcc-488b-4836-94fd-c489f8e1ed7d}  NDIS Helper Class
    {A1E7036D-72A1-4529-B108-0C3C9E92D424}  Create and edit Wired policies
    {B475F925-E3F7-414C-8C72-1CEE64B9D8F6}  PSFactoryBuffer
    {bc65fb43-1958-4349-971a-210290480130}  Ncd Property Page
    {C330DE32-29C7-4cf2-9807-74BCB5486A37}  Nap Client WMI Provider Class
    {D60795C3-F2A5-45b1-A731-2516E7EAB8EB}  NAP Helper Class
    {d6afe216-3106-4e91-953f-ffa26064c8ee}  Nap Config Write Class
    {DCBCA92E-7DBE-4eda-8B7B-3AAEA4DD412B}  Quarantine Private QEC Binding class
    {DD373F1A-7227-4e3c-9AFB-98C288CF1956}  Quarantine EnforcementClient Connection
class
    {e5fae3b3-1ac8-4bd3-87e6-48eff509ddaa}  Nap Certificate Relying Party class
    {ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}  Nap Config Read class
    {eb082ba1-df8a-46be-82f3-35bf9e9be52f}  Quarantine Agent Management class
Tue Jul 14 04:54:30 2009 Z
    {02703d01-d9ab-422c-bbb7-37a0fabc7642}  WCN NCD Pairing Handler Class
    {0273c57c-6693-4444-b20c-a62a3b185b7e}  Device Display Objects Proxies
    {0BD7E521-4DA6-42D5-81BA-1981B6B94075}  PSFactoryBuffer
    {0D0D66EB-CF74-4164-B52F-08344672DD46}  UPnP Service Provider Class
    {145B4335-FE2A-4927-A040-7C35AD3180EF}  SSDP Provider Class
    {1B0D2365-B3A3-4759-9533-D6861E86DE32}  IUninstallProvider_PSFactory
    {1E1DAECB-F640-416d-96A3-2BC8AFDF6059}  IUninstallElevatedHandler_PSFactory
    {2DA6AA7F-8C88-4194-A558-0D36E7FD3E64}  Create and edit Wireless policies
    {35b1d3bb-2d4e-4a7c-9af0-f2f677af7c30}  WNet Provider Class
    {383b69fa-5486-49da-91f5-d63c24c8e9d0}  Device Pairing Handler Class
    {3B2D194D-F107-4489-ABF8-57A125275E4E}  Bluewire General Property Sheet
    {4876DC0E-F963-4227-9A8F-19872B75D231}  Storage Devices Handler
    {5C0D19E4-A364-4ef6-9288-DBD194593879}  Device Center General Property Sheet
    {5F884992-EE6D-418B-9E6C-0C2A0FA94D17}  Device Center Hardware Property Sheet
    {65E6AC96-4B9B-47EA-AF5C-5DFCC72DCE26}  PSFactoryBuffer
    {70799824-b3ba-4157-96cb-a34d6170c96f}  WindowsInfo.xml parser
    {71455ADC-0A77-405F-BF67-EA663D276653}  Bluetooth MTP Devices Menu
    {7754801c-b01d-4d74-84cb-dfd70669ffbe}  DeviceInfo.xml parser
    {8101368E-CABB-4426-ACFF-96C4108120CD}  Plug and Play Provider Class
    {827CE1A1-8255-4165-8C83-8379F8C127AE}  Create and edit Wireless policies
    {89A502FC-857B-4698-A0B7-027192002F9E}  Bluewire Unpairing Handler
    {9197e04d-2b9f-4849-8bf7-75294eb5c043}  User Mode Bus Driver Class
    {A8A91A66-3A7D-4424-8D24-04E180695C7A}  Device Center
    {B8A27942-ADE7-4085-AA6E-4FADC7ADA1EF}  PNPX Pairing Handler Class
    {b8fb4ad7-ea4a-4b47-bfdc-bfc94160a8ea}  Device Display Object Function Discovery
Provider
    {c282ddad-08b1-494e-951f-d32b89024142}  DXP Properties parser
    {C2B136E2-D50E-405C-8784-363C582BF43E}  DeviceCenter Initialization
    {C97FCC79-E628-407D-AE68-A06AD6D8B4D1}  AssociatedDevicePresence Class
    {cee8ccc9-4f6b-4469-a235-5a22869eef03}  PNPX Association Class
```

Page 31

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {d2e86c4f-ea06-4a89-bf00-b49706db46e6} | DDO Resource Info |
| {D3DCB472-7261-43ce-924B-0704BD730D5F} | WS Discovery Provider Class |
| {D88EC52B-8D57-49e1-9EB3-4D267D68A2AE} | Bluewire Elevated Unpairing Handler |
| {DD468E14-AF42-4D63-8908-EDAC4A9E67AE} | Create and edit Wireless policies |
| {f59aa553-8309-46ca-9736-1ac3c62d6031} | Device Display Status Manager |
| {F77C0A7D-7395-45c5-BDFC-B096BF6C4DA0} | Bluewire Paired Devices Menu |

Tue Jul 14 04:54:29 2009 Z

| | |
|---|---|
| {17B75166-928F-417d-9685-64AA135565C1} | Image Transcode |
| {227ec397-6791-4ac6-a762-2f70f99015c2} | IAS Netsh XML Helper |
| {3F30C968-480A-4C6C-862D-EFC0897BB84B} | Photo Extract Image |
| {48da6741-1bf0-4a44-8325-293086c79077} | |
| {5f6c1ba8-5330-422e-a368-572b244d3f87} | PSFactoryBuffer |
| {6BC09692-0CE6-11D1-BAAE-00C04FC2E20D} | IAS Attribute Dictionary |
| {6BC0969D-0CE6-11D1-BAAE-00C04FC2E20D} | |
| {6BC0969F-0CE6-11D1-BAAE-00C04FC2E20D} | |
| {6BC096A0-0CE6-11D1-BAAE-00C04FC2E20D} | |
| {6BC096C6-0CE6-11D1-BAAE-00C04FC2E20D} | |
| {6BC096C8-0CE6-11D1-BAAE-00C04FC2E20D} | |
| {6f13dd2e-ebee-4dd5-a72e-850b2087f5dd} | Microsoft Metadata Policy Layer |
| {83e05bd5-aec1-4e58-ae50-e819c7296f67} | PSFactoryBuffer |
| {8c2031f1-b169-4e7c-9cb0-56f18d7b0c01} | IAS XML Data Store |
| {9d1b93f1-2e5f-4fdb-a95b-dad8d47e28d8} | RPC Helper Class |
| {a38b883c-1682-497e-97b0-0a3a9e801682} | IPropertyStore Handler for Images |
| {BAE86DDD-DC11-421C-B7AB-CC55D1D65C44} | PSFactoryBuffer |
| {BC94D813-4D7F-11d2-A8C9-00AA00A71DCA} | SdoService Class |
| {BED4D415-7971-4310-AA07-6AC15EA06ACC} | WinInet Helper Class |
| {C7657C4A-9F68-40fa-A4DF-96BC08EB3551} | Photo Thumbnail Provider |
| {E9218AE7-9E91-11D1-BF60-0080C7846BC0} | SdoMachine Class |
| {e9970fa4-b6aa-11d9-b032-000d56c25c27} | IAS SDO Helper Class |
| {EAE826D3-ECB5-49ff-BC55-7B318E78C6DD} | Dot3BalloonHandler Class |
| {F1171280-BC35-45d1-8F53-8AB833267899} | DNS Helper Class |

Tue Jul 14 04:54:28 2009 Z

| |
|---|
| {01B90D9A-8209-47F7-9C52-E1244BF50CED} |
| {076C2A6C-F78F-4C46-A723-3583E70876EA} |
| {0E25DC18-9F5E-48B1-80B3-D124E81B773B} |
| {1765E14E-1BD4-462E-B6B1-590BF1262AC6} |
| {22C21F93-7DDB-411C-9B17-C5B7BD064ABC} |
| {6D68D1DE-D432-4B0F-923A-091183A9BDA7} |
| {72B624DF-AE11-4948-A65C-351EB0829419} |
| {7F12E753-FC71-43D7-A51D-92F35977ABB5} |
| {9CB5172B-D600-46BA-AB77-77BB7E3A00D9} |
| {A26CEC36-234C-4950-AE16-E34AACE71D0D} |
| {AA94DCC2-B8B0-4898-B835-000AABD74393} |
| {AC4CE3CB-E1C1-44CD-8215-5A1665509EC2} |
| {C17CABB2-D4A3-47D7-A557-339B2EFBD4F1} |
| {E7E79A30-4F2C-4FAB-8D00-394F2D6BBEBE} |
| {ED822C8C-D6BE-4301-A631-0E1416BAD28F} |

Tue Jul 14 04:54:27 2009 Z

| | |
|---|---|
| {21D6D48E-A88B-11D0-83DD-00AA003CCABD} | TAPI Class |
| {45234E3E-61CC-4311-A3AB-248082554482} | Plug-in Terminal |
| {4C8D0AF0-7BF0-4f33-9117-981A33DBD4E6} | FilePlaybackTerminal Class |
| {4DDB6D36-3BC1-11d2-86F2-006008B0E5D2} | MSP Class |
| {7170F2E0-9BE3-11D0-A009-00AA00B605A4} | TAPI3 Terminal Manager Class |
| {72970BEB-81F8-46D4-B220-D743F4E49C95} | Volume Shadow Copy WMI Provider |
| {890CB943-D715-401B-98B1-CF82DCF36D7C} | Volume Shadow Copy WMI Provider |
| {AC48FFE0-F8C4-11d1-A030-00C04FB6809F} | RequestMakeCall Class |
| {AED6483E-3304-11d2-86F1-006008B0E5D2} | Video Render Dynamic Terminal |
| {AED6483F-3304-11d2-86F1-006008B0E5D2} | Media Streaming Dynamic Terminal |
| {B138E92F-F502-4adc-89D9-134C8E580409} | FileRecordingTerminal Class |
| {BB918E32-2A5C-4986-AB40-1686A034390A} | Plug-in Terminal Class |
| {BCEA735B-4DAC-4B71-9C47-1D560AFD2A9B} | DfsShellAdmin Class |
| {E9225296-C759-11d1-A02B-00C04FB6809F} | DispatchMapper Class |
| {ECCDF543-45CC-11CE-B9BF-0080C87CDBA6} | DfsShell Class |

Page 32

\

SOFTWARE OUTPUT.txt

```
Tue Jul 14 04:54:26 2009 Z
   {02A3586C-D264-40BF-97F7-FE40F7E3A882}  Microsoft Virtual Disk Service Dynamic
Provider
   {0B5A2C52-3EB9-470a-96E2-6C6D4570E40F}  VssSnapshotMgmt Class
   {135698D2-3A37-4d26-99DF-E2BB6AE3AC61}  IVolumeClient3_PSFactory
   {3A410F21-553F-11d1-8E5E-00A0C92C9D5D}  IDMRemoteServer_PSFactory
   {4BDAFC52-FE6A-11d2-93F8-00105A11164A}  IVolumeClient2_PSFactory
   {65EE1DBA-8FF4-4a58-AC1C-3470EE2F376A}  VSSoftwareProvider Class
   {7086AD76-44BD-11D0-81ED-00A0C90FC491}  DiskManagement.UITasks
   {7D1933CB-86F6-4A98-8628-01BE94C9A575}  Virtual Disk Service
   {80CB8C11-0E10-45F4-A1BA-EAD3838D7034}  Microsoft Virtual Disk Service Virtual
Disk Provider
   {8EAD3A12-B2C1-11d0-83AA-00A0C92C9D5D}  DiskManagement.SnapInExtension
   {95243A62-2F9B-4FDF-B437-40D965F6D17F}  VSSRemoteCoordinator Class
   {9C38ED61-D565-4728-AEEE-C80952F0ECDE}  Virtual Disk Service Loader
   {AEB84C83-95DC-11D0-B7FC-B61140119C4A}  DiskManagement.Control
   {D2D79DF5-3400-11d0-B40B-00AA005FF586}  IVolumeClient_PSFactory
   {D2D79DF7-3400-11d0-B40B-00AA005FF586}  IDMNotify_PSFactory
   {DBFCA500-8C31-11D0-AA2C-00A0C92749A3}  DiskManagement.SnapInComponent
   {DE010DA1-289B-4232-8CD0-5112DCA6A7B3}  Microsoft Virtual Disk Service Basic
Provider
   {DEB01010-3A37-4d26-99DF-E2BB6AE3AC61}  IVolumeClient4_PSFactory
   {E0393303-90D4-4A97-AB71-E9B671EE2729}  VDS ProxyStub
   {E13B6686-3F39-11D0-96F6-00A0C9191601}  DiskManagement.SnapIn
   {E13B6688-3F39-11D0-96F6-00A0C9191601}  DiskManagement.DataObject
   {E579AB5F-1CC4-44b4-BED9-DE0991FF0623}  VSSCoordinator Class
   {F2C2787D-95AB-40D4-942D-298F5F757874}  PSFactoryBuffer
   {FAC1D9C0-0296-11D1-A840-00A0C92C9D5D}  DiskManagement.SnapInAbout
Tue Jul 14 04:54:25 2009 Z
   {00020C01-0000-0000-C000-000000000046}  Sound (OLE2)
   {00022601-0000-0000-C000-000000000046}  Media Clip
   {00022602-0000-0000-C000-000000000046}  Video Clip
   {00022603-0000-0000-C000-000000000046}  MIDI Sequence
   {0003000C-0000-0000-C000-000000000046}
   {0003000D-0000-0000-C000-000000000046}  Sound
   {0003000E-0000-0000-C000-000000000046}  Media Clip
   {08d450b7-f7e5-4424-8229-11888adb7c14}
   {0bf754aa-c967-445c-ab3d-d8fda9bae7ef}  SlideshowContextMenu
   {0CD7A5C0-9F37-11CE-AE65-08002B2E1262}  Cabinet Shell Folder
   {1a184871-359e-4f67-aad9-5b9905d62232}  Microsoft Windows Font Context Menu
Handler
   {299D0193-6DAA-11d2-B679-006097DF5BD4}  FTP IDataObject impl
   {35CEC8A3-2BE6-11D2-8773-92E220524153}
   {4f6bcd94-c2a5-42ce-8dbc-31e794be4630}  Shell Computer Accounts
   {56EA1054-1959-467f-BE3B-A2A787C4B6EA}  SHACCT Profile Notification Handler
   {593FB605-4854-4965-B5A1-70AB54AB6475}
   {596AB062-B4D2-4215-9F74-E9109B0A8153}  Previous Versions Property Page
   {59be4990-f85c-11ce-aff7-00aa003ca9f6}  Shell extensions for Microsoft Windows
Network objects
   {63da6ec0-2e98-11cf-8d82-444553540000}  Microsoft FTP Folder
   {68ddbb56-9d1d-4fd9-89c5-c0da2a625392}  UnexpectedShutdownReason
   {730F6CDC-2C86-11D2-8773-92E220524153}  SysTrayInvoker
   {87CB4E0D-2E2F-4235-BC0A-7C62308011F6}  PSFactoryBuffer
   {888DCA60-FC0A-11CF-8F0F-00C04FD7D062}  Compressed (zipped) Folder SendTo Target
   {8a7cae0e-5951-49cb-bf20-ab3fa1e44b01}  Windows Font previewer
   {8E4062D9-FE1B-4b9e-AA16-5E8EEF68F48E}  Registration Control
   {8f3080a6-af99-4f2e-a806-f3d5702a0444}  Shell Computer Groups
   {93412589-74D4-4E4E-AD0E-E0CB621440FD}  Font Settings
   {987D8DFA-3E2C-4929-9C51-61AC8E00CBC3}  Shell Logged On Accounts
   {99CDC6E0-DA00-4dfa-8EB8-831D774F8891}  Shell Profile Accounts
   {9DB7A13C-F208-4981-8353-73CC61AE2783}  Previous Versions
   {a3c3d402-e56c-4033-95f7-4885e80b0111}  Previous Versions Results Delegate Folder
   {B6AFFB50-6F46-49B1-B912-C3F7A876CCCA}
```

Page 33

SOFTWARE OUTPUT.txt
```
  {B8BE1E19-B9E4-4ebb-B7F6-A8FE1B3871E0}  Microsoft Windows Font IExtractImage
Handler
  {b8cdcb65-b1bf-4b42-9428-1dfdb7ee92af}  Compressed (zipped) Folder Context Menu
  {BD472F60-27FA-11cf-B8B4-444553540000}  Compressed (zipped) Folder Right Drag
Handler
  {BD84B380-8CA2-1069-AB1D-08000948F534}  Microsoft Windows Font Folder
  {C3C39131-B182-4801-B437-6D1E65B72F57}  Shell User Accounts
  {d20a3293-3341-4ae8-9aaf-8e397cb63c34}  DefragEngine Class
  {DFE49CFE-CD09-11D2-9643-00C04f79ADF0}  Cabview Data Object
  {E88DCCE0-B7B3-11d1-A9F0-00AA0060FA31}  CompressedFolder
  {ed9d80b9-d157-457b-9192-0e7280313bf0}  Compressed (zipped) Folder DropHandler
  {F20DA720-C02F-11CE-927B-0800095AE340}  Package
  {f8c2ab3b-17bc-41da-9758-339d7dbf2d88}  Previous Versions Results Folder
  {ff609cc7-d34d-4049-a1aa-2293517ffcc6}  SetBackgroundContextMenu
Tue Jul 14 04:54:24 2009 Z
  {0b2c9183-c9fa-4c53-ae21-c900b0c39965}  CLSID_PathCompleteProvider
  {1685D4AB-A51B-4af1-A4E5-CEE87002431D}  CLSID_GrepProvider
  {1C0F439D-7C29-4bde-8952-4EEB6A49E048}  CLSID_GrepWdsResolver
  {25256c24-3b75-49b3-a433-4bb2f8865896}  CLSID_StartMenuProvider
  {30276b4f-f25c-457c-a4b7-08574f8ea528}  CLSID_ResultSetFactory
  {36a479ef-8b67-4d01-8dda-753cfcb2dd96}  CLSID_FilteredItemFactory
  {3722c3b1-82e8-4022-8b27-1f8a68b44ac7}  CLSID_ProviderConfig
  {3B1B5147-715E-49e0-AE9F-ADF86724BB89}  CLSID_DateTimeIntervalGenerator
  {3EA48300-8CF6-101B-84FB-666CCB9BCD32}  OLE Docfile Property Page
  {48E277F6-4E74-4cd6-BA6F-FA4F42898223}  Windows Search OpenSearch Provider
  {4A8ECCAC-181D-4c1b-BF8F-5D52C4008FB9}  Accessing Options for Structured Query
  {4db26476-6787-4046-b836-e8412a9e8a27}  Shared Bitmap Object
  {50EF4544-AC9F-4A8E-B21B-8A26180DB13F}  Local Thumbnail Cache
  {7988B571-EC89-11cf-9C00-00AA00A14F56}  Microsoft Disk Quota
  {7988B573-EC89-11cf-9C00-00AA00A14F56}  Microsoft Disk Quota UI
  {7efc002a-071f-4ce7-b265-f4b4263d2fd2}  Local Thumbnail Cache
  {807e5a10-4856-4f9a-8e3c-a1f7e75648b3}  CLSID_QueryResult
  {8099904b-0b91-4906-a89d-11de2bd8f737}  StartMenu Path Complete Query Cache
  {889900c3-59f3-4c2f-ae21-a409ea01e605}  Shared Bitmap Object
  {96B9DAE3-CF15-45e9-9719-57285348225E}  Windows Search OpenSearch Icon Handler
  {AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}  Thumbnail Cache Class Factory for Out of
Proc Server
  {BD84B381-8CA2-1069-AB1D-08000948F534}  PANOSE Core Mapper
  {daf95313-e44d-46af-be1b-cbacea2c3065}  CLSID_StartMenuProviderFolder
  {db6efb73-5153-43b7-8078-c6ffc4c0238c}  CLSID_CheckCompositionCycles
  {e345f35f-9397-435c-8f95-4e922c26259e}  CLSID_StartMenuPathCompleteProviderFolder
Tue Jul 14 04:54:23 2009 Z
  {05d7b0f4-2121-4eff-bf6b-ed3f69b894d7}  Taskbar Control Panel
  {05d7b0f4-2121-4eff-bf6b-ed3f69b894d8}
  {05d7b0f4-2121-4eff-bf6b-ed3f69b894d9}  Taskbar
  {15fc1bac-8d83-4e87-8cc2-a70c9f66f943}
  {17cd9488-1228-4b2f-88ce-4298e93e0966}  Set User Defaults
  {1968106d-f3b5-44cf-890e-116fcb9ecef1}  Application Registration UI
  {25EC352E-72E1-4724-9A28-4AE730072149}
  {29D365AE-D23B-4004-8658-5ED2A59CD77C}  Shell User Enumeration Object
  {2B6DA137-316E-458B-A0AB-BE48C8EC39B9}  Display Control Panel
  {42071712-76d4-11d1-8b24-00a0c9068ff3}  Display Adapter CPL Extension
  {42071713-76d4-11d1-8b24-00a0c9068ff3}  Display Monitor CPL Extension
  {430da762-8632-4840-bc61-3eeaa078e62e}  Windows Display Settings Data
  {4345A2F4-05F5-48D6-B8A2-99D4A2E7B950}  PSFactoryBuffer
  {5BE4911E-3D99-4546-898D-7EE70201C519}  Shell User Object
  {5D05A4EB-54EA-4B7F-A28D-CE51F6BCBAF2}  Virtual Factory for Display
  {60632754-c523-4b62-b45c-4172da012619}  User Accounts
  {6C8EEC18-8D75-41B2-A177-8831D59D2D50}  Mouse Control Panel
  {725BE8F7-668E-4C7B-8F90-46BDB0936430}  Keyboard Control Panel
  {9b4e5207-9539-4258-b4a0-4e70e9e565ec}  User Accounts Control Panel
  {9C60DE1E-E5FC-40f4-A487-460851A8D915}  AutoPlay
  {C555438B-3C23-4769-A71F-B6D3D9B6053A}  Display
```
Page 34

SOFTWARE OUTPUT.txt

```
{C6D7AB70-3D91-433D-8D9E-E1B52035C47F}
{CE510457-55EC-4f86-91BE-323BC91AC34F}    Shell User Domain Enumeration Object
{D4EFF9CD-16DE-446e-83C5-9537543CF4A1}    Set User Defaults Control Panel
{f92e8c40-3d33-11d2-b1aa-080036a75b03}    Display TroubleShoot CPL Extension
Tue Jul 14 04:54:22 2009 Z
{00A77FF7-A514-493e-B721-CDF8CB0F5B59}    Computer Info Advise
{025A5937-A6BE-4686-A844-36FE4BEC8B6D}    Power Options
{0289a7c5-91bf-4547-81ae-fec91a89dec5}    Microsoft Windows Remote Shell Host
{03C93300-8AB2-41C5-9B79-46127A30E148}    PSFactoryBuffer
{045473BC-A37B-4957-B144-68105411ED8E}    PSFactoryBuffer
{047DEC5A-95C1-4C86-827F-7B8C92EBA67A}    PSFactoryBuffer
{0ce3e86f-d5cd-4525-a766-1abab1a752f5}    SideShowNotification Class
{1C749B87-568C-4865-8E73-6413F8372CE6}    Lpksetup LUA Elevation
{2aa2b5fe-b846-4d07-810c-b21ee45320e3}    Network Provisioning via XML Class
{2EA7A549-7BFF-4aae-BAB0-22D43111DE49}    PSFactoryBuffer
{3F66389B-BA65-4782-BA9D-B66367C8E7F1}    Power Control Panel
{45FD65ED-6BC2-47ae-B391-9E2B79F07C52}    System Control Panel
{500DD1A1-B32A-4a37-9283-1185FB613899}    PSFactoryBuffer
{514B5E31-5596-422F-BE58-D804464683B5}    Region and Language UAC Elevation
{5BFF4E02-D379-4050-A382-C6504A980D46}    PowrProfApi
{62D8ED13-C9D0-4CE8-A914-47DD628FB1B0}    Region and Language
{7A076CE1-4B31-452a-A4F1-0304C8738100}    Network and Sharing Center Cpl Elevated
Virtual Factory
{7C92505F-53A4-4D39-B31C-871D82A907DE}    PSFactoryBuffer
{7DE087A5-5DCB-4df7-BB12-0924AD8FBD9A}    WSMan InternalAutomation Class
{84CCE1D2-97AD-4448-AF0F-A79164073A60}    Personalization Control Panel Element
Provider
{8E908FC9-BECC-40f6-915B-F4CA0E70D03D}    Network and Sharing Center
{90954C68-4D60-4023-A1F8-C6AF6F62E1C8}    Network and Sharing Center
{9678f47f-2435-475c-b24a-4606f8161c16}    Microsoft Windows WSMan Provider Host
{98068995-54d2-4136-9bc9-6dbcb0a4683f}    Microsoft Windows Remote Shell Host With
User Settings
{9A7C3FC6-8C9E-40A8-8CD9-0F3715483825}    PSFactoryBuffer
{9acf41ed-d457-4cc1-941b-ab02c26e4686}    Microsoft Windows WSMan Provider Host With
User Settings
{9df523b0-a6c0-4ea9-b5f1-f4565c3ac8b8}    Date and Time Properties
{a323554a-0fe1-4e49-aee1-6722465d799f}    DateTimeCPL Flyout Class
{BA9BB214-D930-4206-8F8F-BF0F1EAA4A6B}    PSFactoryBuffer
{BB06C0E4-D293-4f75-8A90-CB05B6477EEE}    System
{BBD8C065-5E6C-4e88-BFD7-BE3E6D1C063B}    Virtual Factory for Power Options Control
Panel
{BCED617B-EC03-420b-8508-977DC7A686BD}    WSMan Automation Class
{BF85540E-0DF3-47bc-AC5D-305442704708}
{C0DCC3A6-BE26-4bad-9833-61DFACE1A8DB}    Network Center LUA
{c89e334c-e65f-4156-842e-ea89cec71dea}    WFP and IPsec Helper Class
{DFBBDBF8-18DE-49b8-83DC-EBC727C62D94}    SideShowKeyCollection Class
{e20543b9-f785-4ea2-981e-c4ffa76bbc7c}    SideShowSession Class
{E2E7934B-DCE5-43C4-9576-7FE4F75E7480}    Date and Time Control Panel
{E640F415-539E-4923-96CD-5F093BC250CD}    SideShowPropVariantCollection Class
{f6b13ba7-d626-45e5-82c5-26e596114dc0}    WFP Clients Extensible Helper Class
{F73C1438-71B4-4D91-AD13-1F889A03AC67}    PSFactoryBuffer
Tue Jul 14 04:54:21 2009 Z
{01D0A625-782D-4777-8D4E-547E6457FAD5}    CEIPLuaElevationHelper
{0E3BE0D7-030E-4CA3-A911-D86E24AE0A3C}    TCImeComponentMgr
{0E4EFFC0-2387-11D3-B372-00105A98B7CE}    Microsoft.JScript.JSAuthor
{0E9A7BB5-F699-4D66-8A47-B919F5B6A1DB}    ERC Lua Support
{11D5C91F-0A98-11D1-BB10-00C04FC9A3A3}    Computer Management 1.0 Object
{17A898FB-3FC5-455C-87A9-DB06F9D0A557}    ImeCommonAPIClassFactory
{1C5346B8-63E1-4c2b-B125-3C5DB94E946C}    TC IME7 Dictionary Applet
{20cd9315-87d0-40b4-b925-0a8f208e1f8d}    ImeCommonAPI_KOR_Desktop_V1 Class
{20D04FE0-3AEA-1069-A2D8-08002B30309D}    Computer
{227188db-3179-4fdf-af3a-da3b85a0b3cc}    ImeCommonAPIClassFactory_KOR_Desktop_V1
Class
```

Page 35

```
                              SOFTWARE OUTPUT.txt
     {25ECF786-A925-4706-A269-EEF5AD6899DB}   ImeCommonAPIClassFactory
     {432D76CE-8C9E-4EED-ADDD-91737F27A8CB}   Microsoft.JScript.DebugConvert
     {49FC0B81-206C-407F-9F5B-106E5A3EE2D7}   SCImeComponentMgr
     {4BC67F23-D805-4384-BCA3-6F1EDFF50E2C}   ERCLuaElevationHelper
     {50055B2F-D4FF-42E1-9D8F-5D48F327F3AC}   WERCOM
     {531FDEBF-9B4C-4A43-A2AA-960E8FCDC732}   ImTCTip
     {58221C67-EA27-11CF-ADCF-00AA00A80033}   Computer Management 1.0 Object
     {6A02951C-B129-4D26-AB92-B9CA19BDCA26}   Microsoft.JScript.COMPropertyInfo
     {81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E}   ImSCTip
     {8D9B1EC0-181B-4d6d-987E-2754B506B242}   MS PinYin 5.0 Dictionary Applet
     {95688ffa-250d-49bd-b40a-8ed3a8ef4c8e}   ImeKeyEventHandler Class
     {A028AE76-01B1-46C2-99C4-ACD9858AE02F}   IMKRTIP
     {B71E484D-93ED-4B56-BFB9-CEED5134822B}   Microsoft.JScript.Vsa.VsaEngine
     {C3A43F75-FE02-47d8-B3EE-0B568C0C5043}
     {C7B9C313-2FD4-4384-8571-7ABC08BD17E5}   Microsoft.JScript.COMMethodInfo
     {CA0F511A-FAF2-4942-B9A8-17D5E46514E8}   Microsoft.JScript.COMFieldInfo
     {CA236752-2E77-4386-B63B-0E34774A413D}
     {CACA7238-3C7E-4a25-AD73-DE1A4F8C7214}
     {D01B8F28-0BD1-4652-A415-8229F5EE506C}   PSFactoryBuffer
     {D74A07B1-EA36-4f32-A85A-9777A4AE12AA}   PSFactoryBuffer
     {F407D01A-0BCB-4591-9BD6-EA4A71DF0799}   CHT Language model
Tue Jul 14 04:54:20 2009 Z
     {0095b496-f121-4256-96a0-09179828cc16}   CImeProductObject_JK Class
     {019F7150-E6DB-11D0-83C3-00C04FDDB82E}   Microsoft IME (Japanese)
     {01FE4A1F-CC5C-44AB-A1E6-CFBD9249146D}   PSFactoryBuffer
     {03B5835F-F03C-411B-9CE2-AA23E1171E36}   IMJPTIP
     {17fb3711-de14-477f-8b81-32a9c11a6938}   CImeCommonAPI Class
     {35CC8486-4FB1-11D3-A5DA-00C04F88249B}   Microsoft Korean IME Handwriting Applet
     {3A59A18B-F03C-48C8-8AA7-181D35291FD7}   IIMECheckDefaultInputProfile
     {4BE5C3B3-53A2-4F2F-AF9D-D26A5327EB92}   Microsoft Korean IME 8.0 SKF Applet
     {4C870C20-4ED3-4235-9A2A-7185F8A87D06}   HanjaDic Class
     {6279B7CB-D768-4FBE-A6D5-ADD4F711E53B}   Microsoft IME SingleKanjiDictionary
interface
     {6A91029E-AA49-471B-AEE7-7D332785660D}   Microsoft IME (Japanese)
     {6bdadf65-eb94-419b-907c-0ba9dda7f0df}   CImeRequestSender_JK Class
     {6ffa842b-fd90-4a0e-9315-21c52b2457aa}   CImeKeyMapView_JK Class
     {88c524ca-551b-4c01-9a42-cdb16b745291}   ImeCommonAPI_JPN_Desktop_V1 Class
     {8F0A1029-0DF8-4765-A5FD-16E8ECB3545C}   PSFactoryBuffer
     {91162401-6E6B-478A-A7FF-994EBA35B9C3}   PSFactoryBuffer
     {99a73266-0cdf-4479-88af-1842cbaada22}   IImeIPointSrv wrapper class
     {9f75fdc4-0aba-4866-88a9-75ebb9e7d584}   CImeCommandAvailabilityView_JK Class
     {9FF13758-469B-45A8-8CC7-72182BD7E9BA}   Microsoft IME SKF Applet
     {a38f3677-32fc-4dac-99b3-d804b193d2c4}   ImeKeyEventHandler Class
     {A8C3476D-20E1-4d56-96E7-84E24952228B}   UserDicManager Class
     {af9d2278-060f-4a17-99a9-5044f7f843a8}   CImeProperty_JK Class
     {D26C7A0A-83A0-48D3-9174-529DB999B4A4}   PSFactoryBuffer
     {d54e0450-f515-42ac-bf22-b254a2764d49}
     {DD5CF606-9EA7-49E1-8E82-B789E4443B4F}   MS-IME Handwriting Applet
     {e126b7dd-1c3b-4821-b861-a6da9ce6f096}   ImeCommonAPIClassFactory_JPN_Desktop_V1
Class
Tue Jul 14 04:54:19 2009 Z
     {414AC301-8D95-43C8-99D0-3F25E4076945}   Microsoft Shared Correction UI
     {A3037D66-C043-4F54-91A0-2CDB642E7718}   IMETip
     {CCB1D8CB-D39F-41C9-B793-0196214BDC4E}   IMECFM
Tue Jul 14 04:54:14 2009 Z
     {FD5CD8B1-6FE0-44F3-BBFB-65E3655B096E}
     {FEDB2179-2335-48F1-AA28-5CDA35A2B36D}
Tue Jul 14 04:54:13 2009 Z
     {00B01B2E-B1FE-33A6-AD40-57DE8358DC7D}   System.Security.Cryptography.HMACSHA1
     {01FF4E4B-8AD0-3171-8C82-5C2F48B87E3D}
System.Runtime.Remoting.Metadata.SoapMethodAttribute
     {026CC6D7-34B2-33D5-B551-CA31EB6CE345}   System.Collections.SortedList
     {047a9a40-657e-11d3-8d5b-00104b35e7ef}   Microsoft Common Language Runtime Debugger
```

SOFTWARE OUTPUT.txt

Publisher
{05EBA309-0164-11D3-8729-00C04F79ED0D}  Cor IE Security Manager,
CorIESecurityManager, CorIESecurityManager 1
{06B81C12-A5DA-340D-AFF7-FA1453FBC29A}
System.Security.Policy.AllMembershipCondition
{07F94112-A42E-328B-B508-702EF62BCC29}
System.Runtime.InteropServices.COMException
{08295C62-7462-3633-B35E-7AE68ACA3948}  System.ObsoleteAttribute
{09A60795-31C0-3A79-9250-8D93C74FE540}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapInteger
{0A29FF9E-7F9C-4437-8B11-F424491E3931}  NDP SymBinder
{0A3976C5-4529-4ef8-B0B0-42EED37082CD}  NDP SymReader
{0AE2DEB0-F901-478b-BB9F-881EE8066788}  NDP SymWriter
{0D23F8B4-F2A6-3EFF-9D37-BDF79AC6B440}  System.Reflection.TargetException
{0D52ABE3-3C93-3D94-A744-AC44850BACCD}
System.Collections.Generic.KeyNotFoundException
{0E71F9BD-C109-3352-BD60-14F96D56B6F3}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNormalizedString
{0FF66430-C796-3EE7-902B-166C402CA288}  System.MemberAccessException
{108296C1-281E-11D3-BD22-0000F80849BD}  Pdb based CorSymWriter
{112BC2E7-9EF9-3648-AF9E-45C0D4B89929}  System.TypeLoadException
{11581718-2434-32E3-B559-E86CE9923744}  System.OperationCanceledException
{1163D0CA-2A02-37C1-BF3F-A9B9E9D49245}
System.Runtime.Remoting.Proxies.ProxyAttribute
{146855FA-309F-3D0E-BB3E-DF525F30A715}  System.Collections.Hashtable
{146A47AB-A2CF-3587-BB25-2B286D7566B4}  System.Globalization.NumberFormatInfo
{14910622-09D4-3B4A-8C1E-9991DBDCC553}  System.Diagnostics.StackFrame
{14BE6B21-C682-3A3A-8B24-FEE75B4FF8C5}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtokens
{18B1C7EE-68E3-35BB-9E40-469A223285F7}
System.Runtime.Serialization.OnDeserializedAttribute
{1A06A4DC-E239-3717-89E1-D0683F3A5320}  System.Globalization.KoreanCalendar
{1B979846-AAEB-314B-8E63-D44EF1CB9EFC}
System.Diagnostics.DebuggerStepperBoundaryAttribute
{1C97EF1D-74ED-3D21-84A4-8631D959634A}
System.Runtime.Serialization.OptionalFieldAttribute
{1D09B407-A97F-378A-ACCB-82CA0082F9F3}
System.Runtime.Hosting.ApplicationActivator
{1E66F26B-79EE-11D2-8710-00C04F79ED0D}  Cor MIME Filter, CorFltr, CorFltr 1
{1F17C39C-99D5-37E0-8E98-8F27044BD50A}
System.Security.Cryptography.DSASignatureDeformatter
{1F9F18A3-EFC0-3913-84A5-90678A4A9A80}
System.Security.Cryptography.RijndaelManaged
{20051D1B-321F-3E4D-A3DA-5FBE892F7EC5}  System.Security.Cryptography.HMACRIPEMD160
{204D5A28-46A0-3F04-BD7C-B5672631E57F}
System.Runtime.InteropServices.PreserveSigAttribute
{21F5A790-53EA-3D73-86C3-A5BA6CF65FE9}  System.Runtime.Remoting.ObjRef
{2206D773-CA1C-3258-9456-CEB7706C3710}  System.Globalization.HebrewCalendar
{24540EBC-316E-35D2-80DB-8A535CAF6A35}  System.Runtime.Remoting.RemotingException
{24800CD0-0F4E-4df7-9F69-3C6903C89224}  Microsoft Visual Basic Scripting Engine
{24EEC005-3938-3C71-821D-7F68FD850B2D}
System.Runtime.Remoting.Messaging.RemotingSurrogateSelector
{2763BE6B-F8CF-39D9-A2E8-9E9815C0815E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapIdrefs
{27E986E1-BAEC-3D48-82E4-14169CA8CECF}
System.Threading.ThreadInterruptedException
{27F31D55-D6C6-3676-9D42-C40F3A918636}  System.IO.StringWriter
{2846AE5E-A9FA-36CF-B2D1-6E95596DBDE7}  System.Reflection.AmbiguousMatchException
{29625281-51CE-3F8A-AC4D-E360CACB92E2}
System.Diagnostics.DebuggerNonUserCodeAttribute
{29A6CF6F-D663-31A7-9210-1347871681FC}
System.Security.Permissions.GacIdentityPermission
{29C69707-875F-3678-8F01-283094A2DFB1}  System.CannotUnloadAppDomainException
Page 37

```
                         SOFTWARE OUTPUT.txt
   {29C98DFC-AC6B-4788-BDDD-CA41D6D3704A}  Dia based SymReader
   {2BB6C5E0-C2B9-3608-8868-21CFD6DDB91E}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapNonPositiveInteger
   {2C314899-8F99-3041-A49D-2F6AFC0E6296}  System.Security.Cryptography.HMACSHA256
   {2D5EC63C-1B3E-3EE4-9052-EB0D0303549C}
System.Runtime.InteropServices.SafeArrayTypeMismatchException
   {2DECBCB7-BAC0-316D-9131-43035C5CB480}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapDate
   {30AC0B94-3BDB-3199-8A5D-ECA0C5458381}
System.Runtime.Serialization.OnDeserializingAttribute
   {31C967B5-2F8A-3957-9C6D-34A0731DB36C}  System.Globalization.StringInfo
   {31D353B3-0A0A-3986-9B20-3EC4EE90B389}
System.EnterpriseServices.Internal.ServerWebConfig
   {346D5B9F-45E1-45C0-AADF-1B7D221E9063}
System.EnterpriseServices.Internal.SoapClientImport
   {3495E5FA-2A90-3CA7-B3B5-58736C4441DD}  System.ParamArrayAttribute
   {35E946E4-7CDA-3824-8B24-D799A96309AD}  System.Collections.CaseInsensitiveComparer
   {36DCDA30-DC3B-4D93-BE42-90B2D74C64E7}
System.EnterpriseServices.RegistrationConfig
   {374050DD-6190-3257-8812-8230BF095147}  System.Globalization.JapaneseCalendar
   {390E92C9-FA66-3357-BEF2-45A1F34186B9}
System.Security.Policy.GacMembershipCondition
   {39B68485-6773-3C46-82E9-56D8F0B4570C}  System.Security.Cryptography.MACTripleDES
   {3B0398C9-7812-4007-85CB-18C771F2206F}
System.EnterpriseServices.Internal.ComManagedImportUtil
   {3BD1F243-9BC4-305D-9B1C-0D10C80329FC}  System.ArgumentNullException
   {3C9DCA8B-4410-3143-B801-559553EB6725}  System.Text.UTF7Encoding
   {3CDED51A-86B4-39F0-A12A-5D1FDCED6546}
System.Runtime.Remoting.RemotingTimeoutException
   {3D367908-928F-3C13-8B93-5E1718820F6D}
System.Security.Cryptography.RIPEMD160Managed
   {3DDB2114-9285-30A6-906D-B117640CA927}
System.Security.Policy.ApplicationDirectoryMembershipCondition
   {3E5509F0-1FB9-304D-8174-75D6C9AFE5DA}  System.Threading.ThreadStateException
   {3E8E0F03-D3FD-3A93-BAE0-C74A6494DBCA}  System.AppDomainSetup
   {3F4A4283-6A08-3E90-A976-2C2D3BE4EB0B}  System.Reflection.AssemblyNameProxy
   {3FA7A1C5-812C-3B56-B957-CB14AF670C09}
System.Security.Cryptography.SignatureDescription
   {3FB717AF-9D21-3016-871A-DF817ABDDD51}  System.EventArgs
   {3FDCEEC6-B14B-37E2-BB69-ABC7CA0DA22F}  System.ArgumentException
   {40031115-09D2-3851-A13F-56930BE48038}
System.Security.Cryptography.RNGCryptoServiceProvider
   {405C2D81-315B-3CB0-8442-EF5A38D4C3B8}  System.Diagnostics.StackTrace
   {40AE2088-CE00-33AD-9320-5D201CB46FC9}
System.Diagnostics.SymbolStore.SymDocumentType
   {41970D73-92F6-36D9-874D-3BD0762A0D6F}  System.Diagnostics.DebuggerHiddenAttribute
   {4224AC84-9B11-3561-8923-C893CA77ACBE}  System.SystemException
   {4286FA72-A2FA-3245-8751-D4206070A191}  System.OverflowException
   {433CA926-9887-3541-89CC-5D74D0259144}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapIdref
   {43CD41AD-3B78-3531-9031-3059E0AA64EB}  System.Version
   {44181B13-AE94-3CFB-81D1-37DB59145030}  System.Security.Cryptography.SHA256Managed
   {4479C009-4CC3-39A2-8F92-DFCDF034F748}
System.IO.IsolatedStorage.IsolatedStorageException
   {458AA3B5-265A-4B75-BC05-9BEA4630CF18}
System.EnterpriseServices.Internal.AssemblyLocator
   {4599202D-460F-3FB7-8A1C-C2CC6ED6C7C8}  System.Collections.Stack
   {46080CA7-7CB8-3A55-A72E-8E50ECA4D4FC}
System.Runtime.CompilerServices.CallConvThiscall
   {463AE13F-C7E5-357E-A41C-DF8762FFF85C}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapMonthDay
   {46E97093-B2EC-3787-A9A5-470D1A27417C}  System.DllNotFoundException
   {475E398F-8AFA-43A7-A3BE-F4EF8D6787C9}
                              Page 38
```

SOFTWARE OUTPUT.txt

```
System.Runtime.InteropServices.RegistrationServices
   {477A7D8E-8D26-3959-88F6-F6AB7E7F50CF}   System.Security.Cryptography.HMACSHA512
   {47D3C68D-7D85-3227-A9E7-88451D6BADFC}
System.Collections.CaseInsensitiveHashCodeProvider
   {48728B3F-F7D9-36C1-B3E7-8BF2E63CE1B3}
System.Runtime.Remoting.Channels.TransportHeaders
   {48A75519-CB7A-3D18-B91E-BE62EE842A3E}
System.Threading.SynchronizationLockException
   {48AD62E8-BD40-37F4-8FD7-F7A17478A8E6}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDateTime
   {48C6E96F-A2F3-33E7-BA7F-C8F74866760B}   System.IO.FileNotFoundException
   {48D0CFE7-3128-3D2C-A5B5-8C7B82B4AB4F}
System.Runtime.CompilerServices.MethodImplAttribute
   {4B601364-A04B-38BC-BD38-A18E981324CF}
System.Runtime.CompilerServices.CompilerGlobalScopeAttribute
   {4BE89AC3-603D-36B2-AB9B-9C38866F56D5}
System.Runtime.InteropServices.SafeArrayRankMismatchException
   {4C3EBFD5-FC72-33DC-BC37-9953EB25B8D7}   System.AccessViolationException
   {4C69C54F-9824-38CC-8387-A22DC67E0BAB}
System.Security.Cryptography.X509Certificates.X509Certificate
   {4D187AC2-D815-3B7E-BCEA-8E0BBC702F7C}
System.Security.Cryptography.RSAOAEPKeyExchangeDeformatter
   {4E515531-7A71-3CDD-8078-0A01C85C8F9D}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapName
   {4E77EC8F-51D8-386C-85FE-7DC931B7A8E7}   System.Random
   {4F272C37-F0A8-350C-867B-2C03B2B16B80}
System.Runtime.Serialization.ObjectIDGenerator
   {50369004-DB9A-3A75-BE7A-1D0EF017B9D3}
System.Runtime.Serialization.Formatters.Binary.BinaryFormatter
   {50AAD4C2-61FA-3B1F-8157-5BA3B27AEE61}   System.STAThreadAttribute
   {53A3C917-BB24-3908-B58B-09ECDA99265F}
System.Runtime.Remoting.InternalRemotingServices
   {5520B6D3-6EC6-3CE7-958B-E69FAF6EFF99}
System.Runtime.Remoting.Contexts.SynchronizationAttribute
   {5610F042-FF1D-36D0-996C-68F7A207D1F0}
System.Security.AllowPartiallyTrustedCallersAttribute
   {57154C7C-EDB2-3BFD-A8BA-924C60913EBF}
System.Runtime.Serialization.SerializationException
   {58897D76-EF6C-327A-93F7-6CD66C424E11}   System.MissingMethodException
   {58D052BC-A3DF-3508-AC95-FF297BDC9F0C}   System.IO.EndOfStreamException
   {590E4A07-DAFC-3BE7-A178-DA349BBA980B}
System.Runtime.CompilerServices.IUnknownConstantAttribute
   {5A18D43E-115B-3B8B-8245-9A06B204B717}
System.Diagnostics.SymbolStore.SymLanguageType
   {5B76534C-3ACC-3D52-AA61-D788B134ABE2}
System.Runtime.Remoting.Metadata.SoapFieldAttribute
   {5C35F099-165E-3225-A3A5-564150EA17F5}
System.Runtime.Remoting.Channels.ServerChannelSinkStack
   {5C3E6CE8-B218-3762-883C-91BC987CDC2D}   System.Globalization.JulianCalendar
   {5CA9971B-2DC3-3BC8-847A-5E6D15CBB16E}   System.IndexOutOfRangeException
   {5F3A0F8D-5EF9-3AD5-94E0-53AFF8BCE960}
System.Security.Cryptography.ToBase64Transform
   {5F9A955F-AA55-4127-A32B-33496AA8A44E}
System.EnterpriseServices.Internal.SoapUtility
   {61B3E12B-3586-3A58-A497-7ED7C4C794B9}   System.AppDomainUnloadedException
   {62545937-20A9-3D0F-B04B-322E854EACB0}   System.Security.Policy.Evidence
   {62E92675-CB77-3FC9-8597-1A81A5F18013}
System.Security.Cryptography.RC2CryptoServiceProvider
   {630A3EF1-23C6-31FE-9D25-294E3B3E7486}
System.Runtime.InteropServices.ComRegisterFunctionAttribute
   {647053C3-1879-34D7-AE57-67015C91FC70}   System.ArithmeticException
   {6619A740-8154-43BE-A186-0319578E02DB}   PSFactoryBuffer
   {66CE75D4-0334-3CA6-BCA8-CE9AF28A4396}   System.FlagsAttribute
```

Page 39

SOFTWARE OUTPUT.txt

{673DFE75-9F93-304F-ABA8-D2A86BA87D7C}
System.Security.Cryptography.DSACryptoServiceProvider
{676E1164-752C-3A74-8D3F-BCD32A2026D6}   System.ArrayTypeMismatchException
{682D63B8-1692-31BE-88CD-5CB1F79EDB7B}   System.ApplicationException
{6850404F-D7FB-32BD-8328-C94F66E8C1C7}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNonNegativeInteger
{6896B49D-7AFB-34DC-934E-5ADD38EEEE39}   System.Collections.ArrayList
{68F8AEA9-1968-35B9-8A0E-6FDC637A4F8E}   System.Globalization.GregorianCalendar
{6C1C243A-2146-3342-8078-AC4BFB9DB4E9}
System.EnterpriseServices.CompensatingResourceManager.ClerkMonitor
{6F674828-9081-3B45-BC39-791BD84CCF8F}
System.Security.Cryptography.RSAPKCS1SignatureDeformatter
{6F8527BF-5AAD-3236-B639-A05177332EFE}
System.Runtime.Serialization.OnSerializedAttribute
{6FEF44D0-39E7-4C77-BE8E-C9F8CF988630}   Microsoft Common Language Runtime Debugger
{70A738D1-1BC5-3175-BD42-603E2B82C08B}   System.Globalization.DateTimeFormatInfo
{726BBDF4-6C6D-30F4-B3A0-F14D6AEC08C7}
System.Resources.MissingManifestResourceException
{742AD1FB-B2F0-3681-B4AA-E736A3BCE4E1}
System.Runtime.InteropServices.MarshalDirectiveException
{74BDD0B9-38D7-3FDA-A67E-D404EE684F24}   System.ArgumentOutOfRangeException
{75215200-A2FE-30F6-A34B-8F1A1830358E}   System.UnauthorizedAccessException
{75999EBA-0679-3D43-BDC4-02E4D637F1B1}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapYear
{769B8B68-64F7-3B61-B744-160A9FCC3216}   System.Globalization.TaiwanCalendar
{777F668E-3272-39CD-A8B5-860935A35181}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapToken
{78D22140-40CF-303E-BE96-B3AC0407A34D}
System.Runtime.InteropServices.RuntimeEnvironment
{7AE01D6C-BEE7-38F6-9A86-329D8A917803}
System.Security.SuppressUnmanagedCodeSecurityAttribute
{7AE844F0-ECA8-3F15-AE27-AFA21A2AA6F8}
System.Security.Cryptography.PKCS1MaskGenerationMethod
{7B769B29-35F0-3BDC-AAE9-E99937F6CDEC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapPositiveInteger
{7B938A6F-77BF-351C-A712-69483C91115D}
System.Reflection.InvalidFilterCriteriaException
{7BC115CD-1EE2-3068-894D-E3D3F7632F40}
System.Security.Cryptography.RSAPKCS1SignatureFormatter
{7E3393AB-2AB2-320B-8F6F-EAB6F5CF2CAF}   System.Security.UnverifiableCodeAttribute
{7E34AB89-0684-3B86-8A0F-E638EB4E6252}   System.NotFiniteNumberException
{7F6BCBE5-EB30-370B-9F1B-92A6265AFEDD}   System.InvalidCastException
{7F71DB2D-1EA0-3CAE-8087-26095F5215E6}   System.NullReferenceException
{7F8C7DC5-D8B4-3758-981F-02AF6B42461A}
System.Security.Cryptography.CryptographicException
{7F976B72-4B71-3858-BEE8-8E3A3189A651}   System.Collections.Queue
{7FD3958D-0A14-3001-8074-0D15EAD7F05C}   System.Security.Cryptography.SHA384Managed
{7FE87A55-1321-3D9F-8FEF-CD2F5E8AB2E9}   System.Threading.Overlapped
{81C5FE01-027C-3E1C-98D5-DA9C9862AA21}   System.Object
{837A6733-1675-3BC9-BBF8-13889F84DAF4}
System.Runtime.CompilerServices.DiscardableAttribute
{84589833-40D7-36E2-8545-67A92B97C408}   System.Security.HostSecurityManager
{84F70B6C-D59E-394A-B879-FFCC30DDCAA2}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapLanguage
{8833BC41-DC6B-34B9-A799-682D2554F02F}   System.IO.DirectoryNotFoundException
{88C8A919-EB24-3CCA-84F7-2EA82BB3F3ED}
System.Runtime.Serialization.SurrogateSelector
{89A86E7B-C229-4008-9BAA-2F5C8411D7E0}
System.EnterpriseServices.RegistrationHelper
{89BCC804-53A5-3EB2-A342-6282CC410260}   System.SerializableAttribute
{89D26277-8408-3FC8-BD44-CF5F0E614C82}   System.Security.Policy.PolicyException
{8A3FD229-B2A9-347F-93D2-87F3B7F92753}
System.Runtime.InteropServices.ComConversionLossAttribute

Page 40

```
                              SOFTWARE OUTPUT.txt
    {8C1425C9-A7D3-35CD-8248-928CA52AD49B}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapHexBinary
    {8C40D44A-4EDE-3760-9B61-50255056D3C7}   System.Text.UTF8Encoding
    {8D36569B-14D6-3C3D-B55C-9D02A45BFC3D}   System.MissingFieldException
    {8F45C7FF-1E6E-34C1-A7CC-260985392A05}
System.Runtime.InteropServices.ComUnregisterFunctionAttribute
    {8F6D198C-E66F-3A87-AA3F-F885DD09EA13}
System.Security.Cryptography.DSASignatureFormatter
    {8FD730C1-DD1B-3694-84A1-8CE7159E266B}
System.Runtime.Remoting.Lifetime.LifetimeServices
    {91591469-EFEF-3D63-90F9-88520F0AA1EF}   System.InvalidProgramException
    {9173D971-B142-38A5-8488-D10A9DCF71B0}   System.Threading.ReaderWriterLock
    {91F672A3-6B82-3E04-B2D7-BAC5D6676609}   System.Diagnostics.Debugger
    {92755472-2059-3F96-8938-8AC767B5187B}
System.Security.Cryptography.RSAPKCS1KeyExchangeFormatter
    {92E76A74-2622-3AA9-A3CA-1AE8BD7BC4A8}   System.MethodAccessException
    {93D11DE9-5F6C-354A-A7C5-16CCCA64A9B8}   System.Reflection.ObfuscationAttribute
    {93F551D6-2F9E-301B-BE63-85AEF508CAE0}
System.Diagnostics.DebuggerStepThroughAttribute
    {9546306B-1B68-33AF-80DB-3A9206501515}   System.InvalidOperationException
    {964AA3BD-4B12-3E23-9D7F-99342AFAE812}   System.FormatException
    {96705EE3-F7AB-3E9A-9FB2-AD1D536E901A}   System.ContextStaticAttribute
    {96A058CD-FAF7-386C-85BF-E47F00C81795}   System.Runtime.InteropServices.InAttribute
    {9A3A64F4-8BA5-3DCF-880C-8D3EE06C5538}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapEntities
    {9A944885-EDAF-3A81-A2FF-6A9D5D1ABFC7}
System.Runtime.InteropServices.InvalidOleVariantTypeException
    {9B924EC5-BF13-3A98-8AC0-80877995D403}
System.Runtime.Remoting.Metadata.SoapAttribute
    {9BF86F6E-B0E1-348B-9627-6970672EB3D3}
System.Runtime.Serialization.OnSerializingAttribute
    {9C125A6F-EAE2-3FC1-97A1-C0DCEAB0B5DF}   System.StackOverflowException
    {9C67F424-22DC-3D05-AB36-17EAF95881F2}
System.Runtime.Remoting.Metadata.SoapTypeAttribute
    {9D309F77-4655-372E-84B0-B0FB4030F3B8}
System.Runtime.InteropServices.SetWin32ContextInIDispatchAttribute
    {9DA2F8B8-59F0-3852-B509-0663E3BF643B}   System.MulticastNotSupportedException
    {9E28EF95-9C6F-3A00-B525-36A76178CC9C}   System.Text.ASCIIEncoding
    {9E31421C-2F15-4F35-AD20-66FB9D4CD428}
System.EnterpriseServices.RegistrationHelperTx
    {9EA60ECA-3DCD-340F-8E95-67845D185999}   System.Security.Cryptography.CryptoConfig
    {A0E2E749-63CE-3651-8F4F-F5F996344C32}
System.Security.Cryptography.RSAOAEPKeyExchangeFormatter
    {A0F5F5DC-337B-38D7-B1A3-FB1B95666BBF}   System.Text.UnicodeEncoding
    {A164C0BF-67AE-3C7E-BC05-BFE24A8CDB62}   System.IO.IOException
    {A1C0A095-DF97-3441-BFC1-C9F194E494DB}   System.Exception
    {A36738B5-FA8F-3316-A929-68099A32B43B}   System.PlatformNotSupportedException
    {A36E4EAF-EA3F-30A6-906D-374BBF7903B1}   System.Runtime.Remoting.Contexts.Context
    {A3A1F076-1FA7-3A26-886D-8841CB45382F}
System.Runtime.CompilerServices.CallConvCdecl
    {A5448B7A-AA07-3C56-B42B-7D881FA10934}   System.Security.Policy.ApplicationTrust
    {A6673C32-3943-3BBB-B476-C09A0EC0BCD6}   System.Security.Cryptography.SHA512Managed
    {A7136BDF-B141-3913-9D1C-9BC5AFF21470}
System.Runtime.Remoting.Metadata.W3CXsd2001.SoapYearMonth
    {A7248EC6-A8A5-3D07-890E-6107F8C247E5}
System.Runtime.InteropServices.InvalidComObjectException
    {A7EDDCB5-6043-3988-921C-25E3DEE6322B}   System.Security.Cryptography.HMACMD5
    {A8D058C4-D923-3859-9490-D3888FC90439}
System.Runtime.Serialization.Formatters.SoapFault
    {A8F03BE3-EDB7-4972-821F-AF6F8EA34884}   WmiSecurityHelper Class
    {A8F9F740-70C9-30A7-937C-59785A9BB5A4}   System.IO.DriveNotFoundException
    {AA544D41-28CB-11D3-BD22-0000F80849BD}   SymBinder
    {AAD4BDD3-81AA-3ABC-B53B-D904D25BC01E}   System.DataMisalignedException
                                Page 41
```

SOFTWARE OUTPUT.txt
```
{AB558A90-77EC-3C9A-A7E3-7B2260890A84}
System.EnterpriseServices.CompensatingResourceManager.Compensator
    {AD326409-BF80-3E0C-BA6F-EE2C33B675A5}    System.EntryPointNotFoundException
    {AD664904-FE8A-3217-BBF5-E6AB1D998F5F}
System.Security.Permissions.HostProtectionAttribute
    {AE53ED01-CAB4-39CE-854A-8BF544EEEC35}    System.Security.Cryptography.HMACSHA384
    {AF60343F-6C7B-3761-839F-0C44E3CA06DA}    System.Security.Cryptography.CspParameters
    {AF8C5F8A-9999-3E92-BB41-C5F4955174CD}    System.IO.FileLoadException
    {AFAEF10F-1BC4-351F-886A-878A265C1862}    System.Security.Policy.TrustManagerContext
    {AFC681CF-E82F-361A-8280-CF4E1F844C3E}
System.Runtime.InteropServices.ExternalException
    {AFEF65AD-4577-447A-A148-83ACADD3D4B9}    System.Data.SqlClient.SQLDebugging
    {B0F64827-79BB-3163-B1AB-A2EA0E1FDA23}
System.EnterpriseServices.Internal.ComSoapPublishError
    {B406AC70-4D7E-3D24-B241-AEAEAC343BD9}    System.MTAThreadAttribute
    {B54E38F8-17FF-3D0A-9FF3-5E662DE2055F}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNotation
    {B6EB52D5-BB1C-3380-8BCA-345FF43F4B04}
System.Security.Cryptography.DESCryptoServiceProvider
    {B81CB5ED-E654-399F-9698-C83C50665786}
System.Runtime.InteropServices.OptionalAttribute
    {BC5062B6-79E8-3F19-A87E-F9DAF826960C}
System.Runtime.Remoting.Services.EnterpriseServicesHelper
    {BCB67D4D-2096-36BE-974C-A003FC95041B}
System.Runtime.CompilerServices.CallConvStdcall
    {BDA7BEE5-85F1-3B66-B610-DDF1D5898006}    System.FieldAccessException
    {C016A313-9606-36D3-A823-33EBF5006189}    System.IO.PathTooLongException
    {C03880A5-0B5E-39AD-954A-CE0DCBD5EF7D}    System.AppDomainManager
    {C1ABB475-F198-39D5-BF8D-330BC7189661}
System.Security.Cryptography.FromBase64Transform
    {C30ABD41-7B5A-3D10-A6EF-56862E2979B6}
System.Runtime.Remoting.Messaging.OneWayAttribute
    {C41D0B30-A518-3093-A18F-364AF9E71EB7}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNegativeInteger
    {C41FA05C-8A7A-3157-8166-4104BB4925BA}
System.Security.Cryptography.CryptographicUnexpectedOperationException
    {C437AB2E-865B-321D-BA15-0C8EC4CA119B}
System.Runtime.CompilerServices.NativeCppClassAttribute
    {C498F2D9-A77C-3D4B-A1A5-12CC7B99115D}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtoken
    {C76B435D-86C2-30FD-9329-E2603246095C}
System.Runtime.Remoting.Metadata.SoapParameterAttribute
    {C9F0A842-3CE1-338F-A1D4-6D7BB397BDAA}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDay
    {C9F61CBD-287F-3D24-9FEB-2C3F347CF570}    System.RankException
    {CA35CB3D-0357-11D3-8729-00C04F79ED0D}    Microsoft.IE.Manager
    {CA805B13-468C-3A22-BF9A-818E97EFA6B7}
System.Runtime.InteropServices.SEHException
    {CAA817CC-0C04-4D22-A05C-2B7E162F4E8F}
System.EnterpriseServices.Internal.SoapServerVRoot
    {CAEC7D4F-0B02-3579-943F-821738EE78CC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapMonth
    {CBEAA915-4D2C-3F77-98E8-A258B0FD3CEF}    System.ContextMarshalException
    {CC20C6DF-A054-3F09-A5F5-A3B5A25F4CE6}    System.DuplicateWaitObjectException
    {CC77F5F3-222D-3586-88C3-410477A3B65D}    System.NonSerializedAttribute
    {CCF306AE-33BD-3003-9CCE-DAF5BEFEF611}    System.OutOfMemoryException
    {CDC70043-D56B-3799-B7BD-6113BBCA160A}    System.MissingMemberException
    {CDFA7117-B2A4-3A3F-B393-BC19D44F9749}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapAnyUri
    {CF8F7FCF-94FE-3516-90E9-C103156DD2D5}
System.Runtime.Serialization.Formatters.InternalRM
    {D049DC2B-82C3-3350-A1CC-BF69FEE3825E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapTime
```
Page 42

```
                          SOFTWARE OUTPUT.txt
   {D13B741D-051F-322F-93AA-1367A3C8AAFB}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNcName
   {D23D2F41-1D69-3E03-A275-32AE381223AC}
System.Runtime.Serialization.FormatterConverter
   {D2548BF2-801A-36AF-8800-1F11FBF54361}
System.Security.Cryptography.MD5CryptoServiceProvider
   {D2EAA715-DAC7-4771-AF5C-931611A1853C}   WmiSinkDemultiplexor Class
   {D41969A6-C394-34B9-BD24-DD408F39F261}
System.Resources.MissingSatelliteAssemblyException
   {D5CB383D-99F4-3C7E-A9C3-85B53661448F}
System.Reflection.CustomAttributeFormatException
   {D6D2034D-5F67-30D7-9CC5-452F2C46694F}   System.TypeUnloadedException
   {D74D613D-F27F-311B-A9A3-27EBC63A1A5D}   System.Threading.Mutex
   {D8013EEF-730B-45E2-BA24-874B7242C425}   System.EnterpriseServices.Internal.Publish
   {D8013EF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.IISVirtualRoot
   {D8013FF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.GenerateMetadata
   {D8A4F3EB-E7EC-3620-831A-B052A67C9944}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapQName
   {D9035152-6B1F-33E3-86F4-411CD21CDE0E}
System.Security.Cryptography.RSACryptoServiceProvider
   {DA317BE2-1A0D-37B3-83F2-A0F32787FC67}
System.Reflection.TargetParameterCountException
   {DAA132BF-1170-3D8B-A0EF-E2F55A68A91D}
System.Security.Cryptography.TripleDESCryptoServiceProvider
   {DAFB2462-2A5B-3818-B17E-602984FE1BB0}   System.NotSupportedException
   {DB13821E-9835-3958-8539-1E021399AB6C}   System.Runtime.Remoting.ServerException
   {DC5DA001-7CD4-11D2-8ED9-D8C857F98FE3}   Cor Remote Loader, CorLoad, CorLoad 1
   {DD5856E5-8151-3334-B8E9-07CB152B20A4}
System.Runtime.Remoting.Channels.ClientChannelSinkStack
   {DE47D9CF-0107-3D66-93E9-A8ACB06B4583}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDuration
   {DFD888A7-A6B0-3B1B-985E-4CDAB0E4C17D}
System.Diagnostics.SymbolStore.SymLanguageVendor
   {E38DA416-8050-3786-8201-46F187C15213}   System.Security.XmlSyntaxException
   {E724B749-18D6-36AB-9F6D-09C36D9C6016}   System.Text.StringBuilder
   {E772BBE6-CB52-3C19-876A-D1BFA2305F4E}
System.Runtime.Serialization.Formatters.SoapMessage
   {E786FB32-B659-3D96-94C4-E1A9FC037868}   System.ExecutionEngineException
   {E7D574D5-2E51-3400-9FB6-A058F2D5B8AB}
System.EnterpriseServices.Internal.ClientRemotingConfig
   {E822F35C-DDC2-3FB2-9768-A2AEBCED7C40}
System.Runtime.Remoting.Services.TrackingServices
   {E9148312-A9BF-3A45-BBCA-350967FD78F5}   System.BadImageFormatException
   {E947A0B0-D47F-3AA3-9B77-4624E0F3ACA4}
System.Runtime.CompilerServices.IDispatchConstantAttribute
   {EAA78D4A-20A3-3FDE-AB72-D3D55E3AEFE6}   System.TimeoutException
   {EBAA029C-01C0-32B6-AAE6-FE21ADFC3E5D}   System.Security.VerificationException
   {EC3DAC94-DF80-3017-B381-B13DCED6C4D8}   System.Globalization.ThaiBuddhistCalendar
   {ECABAFD1-7F19-11D2-978E-0000F8757E2A}
System.EnterpriseServices.Internal.ClrObjectFactory
   {ECC82A10-B731-3A01-8A17-AC0DDD7666CF}   System.Security.HostProtectionException
   {ED0BC45C-2438-31A9-BBB6-E2A3B5916419}
System.Runtime.CompilerServices.CallConvFastcall
   {EE24A2C3-3AA2-33DA-8731-A4FCC1105813}   System.Security.Policy.GacInstalled
   {EE832CE3-06CA-33EF-8F01-61C7C218BD7E}   System.Globalization.HijriCalendar
   {EE96F4E1-377E-315C-AEF5-874DC8C7A2AA}
System.Security.Cryptography.RSAPKCS1KeyExchangeDeformatter
   {EEF05C76-5C98-3685-A69C-6E1A26A7F846}   System.Security.SecurityException
   {EF24F689-14F8-4D92-B4AF-D7B1F0E70FD4}
System.EnterpriseServices.Internal.AppDomainHelper
   {F00CA7A7-4B8D-3F2F-A5F2-CE4A4478B39C}
```

Page 43

SOFTWARE OUTPUT.txt
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapEntity
    {F12FDE6A-9394-3C32-8E4D-F3D470947284}  System.Reflection.AssemblyName
    {F1C3BF79-C3E4-11D3-88E7-00902754C43A}
System.Runtime.InteropServices.TypeLibConverter
    {F1EBA909-6621-346D-9CE2-39F266C9D011}
System.Runtime.InteropServices.ComImportAttribute
    {F59D514C-F200-319F-BF3F-9E4E23B2848C}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapBase64Binary
    {F5E692D9-8A87-349D-9657-F96E5799D2F4}  System.IO.MemoryStream
    {F6914A11-D95D-324F-BA0F-39A374625290}  System.DivideByZeroException
    {F6B6768F-F99E-4152-8ED2-0412F78517FB}
System.EnterpriseServices.Internal.SoapServerTlb
    {F8BE2AD5-4E99-3E00-B10E-7C54D31C1C1D}  System.NotImplementedException
    {FA0B54D5-F221-3648-A20C-F67A96F4A207}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapId
    {FC13A7D5-E2B3-37BA-B807-7FA6238284D5}
System.Security.Cryptography.SHA1CryptoServiceProvider
    {FD8C8FCE-4F85-36B2-B8E8-F5A183654539}
System.Runtime.Remoting.Lifetime.ClientSponsor
    {FDB2DC94-B5A0-3702-AE84-BBFA752ACB36}
System.Runtime.InteropServices.OutAttribute
    {FDF9C30D-CCAB-3E2D-B584-9E24CE8038E3}  System.Security.Cryptography.SHA1Managed
    {FFC9F9AE-E87A-3252-8E25-B22423A40065}  System.ThreadStaticAttribute
Tue Jul 14 04:54:11 2009 Z
    {60254CA5-953B-11CF-8C96-00AA00B8708C}  Shell Extension For Windows Script Host
    {7E48C5CF-72F6-4C84-9F43-B04B87B31243}  Scripting.Signer
    {8066FB71-AFA1-343E-8070-44AB4F3F85C9}
    {88E729D6-BDC1-11D1-BD2A-00C04FB9603F}  Folder Redirection Editor
    {90F1A06E-7712-4762-86B5-7A5EBA6BDB01}  Microsoft Common Language Runtime Meta
Data V2
    {90F1A06E-7712-4762-86B5-7A5EBA6BDB02}  Microsoft Common Language Runtime Meta
Data V2
    {92BDB7E4-F28B-46A0-B551-45A52BDD5125}  PSFactoryBuffer
    {9C86F320-DEE3-4DD1-B972-A303F26B061E}  PSFactoryBuffer
    {B81FF171-20F3-11d2-8DCC-00A0C9B00525}  Type name parser and builder
    {C40D66A0-E90C-46C6-AA3B-473E38C72BF2}  Folder Redirection Editor
    {C89AC250-E18A-4FC7-ABD5-B8897B6A78A5}
System.EnterpriseServices.RegistrationHelperTx
Tue Jul 14 04:54:10 2009 Z
    {0c9ac398-8c78-4b4b-b8c6-675ed1b734a1}  IP Route Helper Class
    {0cdb500e-123f-4e98-b446-0f3eae3c7ebc}  NetBt Helper Class
    {0f3ed1f2-afdd-4b0c-b6d9-229c1bc58a08}  IP Path Helper Class
    {1b9f2bf2-27f5-4dec-a175-3cf7bb8cfd3e}  IP Address Helper Class
    {1e887b90-7201-431d-820e-36aa566e52f4}  Tcp Window Scaling Helper Class
    {1e94e93c-852d-47fb-9197-7edeb41101b0}  IPHTTPS Helper Class
    {25983561-9D65-49CE-B335-40630D901227}  Microsoft IMAPI v2, Raw CD Image Creator
    {27354124-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Stream interleave
utility
    {27354125-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Stream concatenation
utility
    {27354126-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, PRNG based stream
    {27354127-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Zero Stream
    {27354128-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, RAW Disc-At-Once CD
Writer
    {27354129-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Audio CD Writer
    {2735412A-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Standard Data Writer
    {2735412B-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Media Erase
    {2735412C-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Write Engine
    {2735412D-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, CD DVD Device Object
    {2735412E-7F64-5B0F-8F00-5D77AFBE261E}  Microsoft IMAPI v2, Disc Master
    {27354130-7F64-5B0F-8F00-5D77AFBE261E}  PSFactoryBuffer
    {286AA738-2928-49af-A410-4118F5C31626}  Dot3 Helper Class
    {2959380c-1567-40ec-80b0-05907ad6f9de}  IP Neighbor Helper Class
Page 44

```
                       SOFTWARE OUTPUT.txt
{2C941FC5-975B-59BE-A960-9A2A262853A5}  FileSystemImage Class
{2C941FCE-975B-59BE-A960-9A2A262853A5}  BootOptions Class
{2C941FD4-975B-59BE-A960-9A2A262853A5}  PSFactoryBuffer
{30655864-f8cd-45f9-b7d6-6721acb69c5e}  Network Connection Helper Class
{4FDBC3E5-7121-4487-AB95-B58EC04648DB}  Extensible Media Manager Helper Class
{520CCA61-51A5-11D3-9144-00104BA11C5E}  Microsoft IMAPI Disc Recorder
{520CCA63-51A5-11D3-9144-00104BA11C5E}  Microsoft IMAPI Disc Master
{6D54E523-3B26-41CB-9478-BAECBC255189}  SPPCCHandler Class
{73257e95-0378-49d6-a954-44aabc841eab}  Address Acquisition Helper Class
{862321c3-70b2-4ee2-8231-87ec05819d98}  Transport Connection Helper Class
{8A03567A-63CB-4BA8-BAF6-52119816D1EF}  Microsoft IMAPI Disc Recorder Enumerator
{B0DDD260-9E44-4bf2-8602-6D9CE1D0B94F}  UCM Helper Class
{b11d16d0-e195-4ca6-bbd5-1254ec098953}  6To4 Helper Class
{bd69ecaa-ae5c-40d0-b968-7848f3778f56}  DHCP Module Helper Class
{CEEE3B62-8F56-4056-869B-EF16917E3EFC}  Microsoft IMAPI v2, .ISO Image Manager
utility
{EFB92EFB-9236-4bd7-B60D-51D1C7D1C87A}  Framing Layer Helper Class
{FE217CB2-0B2C-48c9-90CA-8D8BCA79248D}  Teredo Helper Class
Tue Jul 14 04:54:09 2009 Z
{00BC7EAE-28D5-4310-BE9F-11526A7FA37F}  ModemActivation Class
{0A14D3FF-EC53-450f-AA30-FFBC55BE26A2}  TokenActivation Class
{179CC917-3A82-40E7-9F8C-2FC8A3D2212B}  SPPLUAObject Class
{32be5ed2-5c86-480f-a914-0ff8885a1b3f}  RDPViewer Class
{6ACB028E-48C0-4A44-964C-E14567C578BA}  SppWmiProvider
{7DA49535-DB7D-47d5-9552-6DAEFA831E64}
{8A99553A-7971-4445-93B5-AAA43D1433C5}  OfflineActivation Class
{91ECFDB4-2606-43E4-8F86-E25B0CB01F1E}  ElevationConfig Class
{9B78F0E6-3E05-4A5B-B2E8-E743A8956B65}  RDPSession Class
{A49211A1-022F-43D7-BC55-D787C66ACF8E}  LicensingPackage Class
{A4DDCA2B-E73C-40C5-83B1-9F40269D0B0D}  OnlineActivation Class
{A6C13C9D-54E1-44FC-82F0-DBE2C843E51A}  SPPUIObject Class
{AA04CA0B-7597-4F3E-99A8-36712D13D676}  LicensingStateTools Class
{b3179149-2b99-48b2-b44b-11aa2034c1a3}  CCNGProvider
{b6dc98b1-0bec-45e1-b2e4-3a2d943f0be4}  CDPAPIProvider
{CB6E2B90-25FA-4F08-B46C-696F5A2B6CA5}  SppWmiTokenActivationSigner
{CD8534F7-B1CE-4A6B-B7CD-AA4AE578A20A}  LicensingStatusData Class
{e5899c7c-0fc7-499e-a262-174fd692dc9f}  CCAPIProvider
{F87B28F1-DA9A-4F35-8EC0-800EFCF26B83}  SPPUIObjectInteractive Class
{f91b9abc-985b-4c04-b5e7-9c7099fc2cda}  CADProvider
{ff8a71c2-7eb8-418b-950d-3b49f43f024f}  CWinCredProvider
Tue Jul 14 04:54:08 2009 Z
{6377013E-2C35-40F3-B8E1-1AB47D12982B}  WABSyncProvider
{6E582707-CCAF-4333-A9B9-3B4F75C362E0}  DeviceOwnershipControl Class
{8373ce97-72b7-4fb2-b5e8-b38aa083d734}  WinSync Anchor Provider Wrapper
{896C2B1D-3586-4FA5-B419-41F4A6D38CF1}  SyncInfrastructureControl Class
{a10dfc9e-ff12-4e7f-bc74-8fe9053920f0}  WinSync Full Enumeration Provider Wrapper
{A38F4597-F640-4189-982F-132ECF8202FA}  WPDSyncProvider Class
{a4a8d991-cc85-493e-ae66-9a847402dad9}  FD Device Pairing Configuration
{a4a8d991-cc85-493e-ae66-9a847402dada}  Device Pairing Config Proxy
{c27f6b1d-fe0b-45e4-9257-38799fa69bc8}  UsbCeip
{C947D50F-378E-4FF6-8835-FCB50305244D}  SyncInfrastructure Class
{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}  Sync Registration
{F9EBBF2D-0C5D-4BF1-AE24-A30F7796D178}  PSFactoryBuffer
{FF3AE31D-55B0-4945-BDE9-622ABB334C1A}  WABSyncConfigUI
Tue Jul 14 04:54:07 2009 Z
{25B25D91-69A2-47fa-A375-FDC98189A06F}
{28803F59-3A75-4058-995F-4EE5503B023C}  Bluetooth Devices
{347CBD95-DD80-4144-81AF-AE803E633A00}  PSFactoryBuffer
{42060D27-CA53-41f5-96E4-B1E8169308A6}  ReliabilityAnalysisCustomHandler
{5F02227D-BF38-48BE-B01A-A47D3006DFA2}  WPDDispatchFactory Class
{8FD8B88D-30E1-4F25-AC2B-553D3D65F0EA}  DXP
{AEE2420F-D50E-405C-8784-363C582BF45A}  DevicePairingFolder Initialization
{b8f87e75-d1d5-446b-931c-3f61b97bca7a}
                            Page 45
```

```
                      SOFTWARE OUTPUT.txt
{D0520B5D-1B5F-4ECF-A940-6E57476AE4B0}
{D7C3453E-1F1C-48CD-AFE6-CFF2A937D337}
{DC79A5C8-CCAD-4698-9034-C4C8068011C5}   PSFactoryBuffer
{E2E5A310-ECED-444F-81D7-ACCA6AC8A1A8}   Win32_TpmProvider Class
{F022A390-2F1E-44d2-AA0A-0FEB28AE6517}   DXP
{F1EFACAA-08A1-461B-9D28-7AA8947889A0}
Tue Jul 14 04:54:06 2009 Z
{022B358F-06B8-4E0D-ADD9-655A8F1E9EDD}
{04DA8451-7F63-4870-A4D7-F55BE66BFDFB}
{05C9DA2B-6DFF-42C7-81CC-706DAE08BC7A}
{095D3BE1-A874-46A5-B989-AE43E3427E3C}
{0D722F1A-9FCF-4E62-96D8-6DF8F01A26AA}   SpShortcut Class
{0E1EEFB2-E336-481C-B178-36261EC5A843}
{0F0549A6-C2E0-442A-85D7-20E3DB9B6A1F}
{0F92030A-CBFD-4AB8-A164-FF5985547FF6}   SpTextSelectionInformation Class
{10A2BDBC-7130-420C-9320-A92CC1919206}
{12D73610-A1C9-11D3-BC90-00C04F72DF9F}   SpITNProcessor Class
{136E0057-D7ED-4B85-9F62-1318CFE1573B}
{1A3ED173-B201-4470-9FC6-EC46CF8D56F1}
{1B2AFB92-0B5E-4A30-B5CC-353DB4F9E150}   SpSapiServer Class
{1B57B2A1-E763-4676-9064-297F1B413632}   SpMMAudioInLegacy Class
{1C0D39B2-C788-40D2-B062-FDF8293D7BC6}
{1D49F57D-47D2-4AEE-A69B-593EC558773F}
{1E69A8EB-0B11-40C3-AC27-906ED77CD946}
{212ADF89-1F86-49D0-914A-DF6C5613C81E}
{2652B813-2260-4EF3-A311-74A7AC6513D7}
{2C9F6BEB-C5B0-42B6-A5EE-84C24DC0D8EF}
{2CB6CDA4-1C14-4392-A8EC-81EEF1F2E079}
{2CB861BB-B1B4-4E14-A1A7-D3FB30C3F5CF}
{2D12DD17-6C4E-456E-A953-D210E3C64176}   SpCommunicator Class
{333E6924-4353-4934-A7BE-5FB5BDDDB2D6}
{3BEE4890-4FE9-4A37-8C1E-5E7E12791C1F}   SpSharedRecognizer Class
{3D0B8752-68F8-4F39-929D-DE20ED323F45}
{3D5DF14F-649F-4CBC-853D-F18FEDE9CF5D}
{3FAA93F3-79FB-4319-8387-B8FFE074FBDA}
{41B89B6B-9399-11D2-9623-00C04F8EE628}   SpInprocRecognizer Class
{42001A23-ED2A-4582-8BCC-6320C543E102}
{4495524E-2E54-472D-86D7-D671CA588F01}
{45EACA36-DBE9-4E4A-A26D-5C201902346D}
{47206204-5ECA-11D2-960F-00C04F8EE628}   SpSharedRecoContext Class
{483B0283-25DB-4C92-9C15-A65925CB95CE}
{49C69FAB-ED5E-4D48-9A65-E4816E5FE642}
{52BE2F87-1638-408A-9A98-74239B0B7DB5}
{530CC6A4-357F-49E2-AB11-3C481DBEDE31}
{53DA1CBB-0F45-46A4-AA6E-47CAAD84C921}
{55DFB4F7-4175-4B3B-B247-D9B399ADB119}   MSTTS Frontend Class (ENU)
{5F104B61-7998-4049-A7BB-C99EFB6B4A4E}
{610133F4-ED38-42E7-9C18-EB2A8F76B99A}
{61A48126-EF74-4D4A-9DDA-43FD542CAD1E}
{61DBD86A-8D1A-4EB0-907C-E4C1BBC8F09A}
{65170AE4-0AD2-4FA5-B3BA-7CD73E2DA825}
{68DC71DC-2327-4040-8F03-50D6A9805049}
{697E2FF0-7FA8-49F1-BB4A-E1D115AA2BBB}
{69ED626B-904D-4DEF-B919-9EF7E4E339DD}
{6C53A912-47C6-4959-B342-DF6C9DA9D494}
{70878DCD-56F6-4681-BC52-BC7F58EDF723}
{712720F4-F4FF-46CF-B6EC-2CC24FC873A5}
{73AD6842-ACE0-45E8-A4DD-8795881A2C2A}   SpInProcRecoContext Class
{773229CD-D53C-4211-ACD8-8F2C7BF2AE7C}
{776266FF-0DC5-4F45-BADA-39A7586FACE2}
{777B6BBD-2FF2-11D3-88FE-00C04F8EF9B5}   SpPhraseBuilder Class
{7AE7416D-AD97-4A4B-B5AC-B3CA7865AFBE}
{7E352021-69D6-4553-86AC-430B0D8FF913}
                      Page 46
```

SOFTWARE OUTPUT.txt

```
{7EFD3C7E-9E4B-4A93-9503-DECD74C0AC6D}
{81442F68-A942-457E-9AF0-C6977E244A7C}
{818C68B0-D4C9-475C-B2CF-AF4242F27C8D}
{86781CF9-799C-4CFF-9AA5-43F4C23FF866}
{874131cb-4ecc-443b-8948-746b89595d20}    WMSpeech Decoder DMO
{87824713-C8B0-4379-8556-1689764E4237}
{89EA5B5A-D01C-4560-A874-9FC92AFB0EFA}
{89F38560-A0AE-4D8C-9E8F-83D4DB8A9F85}
{8A899610-150A-40DB-B57A-940EDB3203CE}
{8B3302D7-95F6-4BC5-A06A-0D6DEF15DB69}
{8E67B6EF-205D-490F-A004-7B04F8F65B62}
{92F2118A-E813-4A4D-9DE2-F96A9DC02C53}
{9CDAEA40-A7D3-4cc5-AED0-B5E35AD0F169}    SpW3CSemanticInterpretation Class
{9D0EAB8C-8EF4-4020-B867-2B1E04E4B8E5}
{9DAA54E8-CD95-4107-8E7F-BA3F24732D95}
{9FE6E853-B35F-4FE4-B006-33148455093E}
{A0A5A274-A190-4A81-997B-9593D6F6D462}
{A25A5CCD-80F4-4E02-AADD-7F39CC55E737}
{A9C6B8DD-3CBB-44CB-AA44-4B1C0DBB404D}
{B1E29D59-A675-11D2-8302-00C04F8EE6C0}    SpGrammarCompiler Class
{B675B948-FBA8-46A4-A4C7-D4291785127B}
{C23FC28D-C55F-4720-8B32-91F73C2BD5D1}    SpPhraseInfoBuilder Class
{C28DA8E5-39C2-4F62-82FA-C61D39A196DF}
{C4BF21DA-F1E5-4C7F-A611-2698645B19EF}
{C700F6EF-A80F-4B24-922A-32308B6FF0C3}
{CA0AC604-8EF2-448A-AE97-62A2C2CC3C46}    SpDMOAudioIn Class
{CF3D2E50-53F2-11D2-960C-00C04F8EE628}    SpMMAudioIn Class
{D0458F37-2228-4FC7-9E66-34133DF4C929}
{D2C13906-51EF-454e-BC67-A52475FF074C}    SpW3CGrammarCompiler Class
{D36D2090-4DF3-4bd4-A22F-0D91975F7964}    SpMSSemanticInterpretation Class
{D385FDAD-D394-4812-9CEC-C6575C0B2B38}
{D6AD10F3-70AB-41E1-96B3-4C36E35D333C}    SpRecoMaster Class
{D9581C03-9766-45A6-B970-1EABBE985986}
{DA93E903-C843-11D2-A084-00C04F8EF9B5}    SpGramCompBackEnd Class
{DC4701DE-1014-44CC-85A6-253F2B30FB9E}
{DC626A64-D684-4627-83CB-44420ABDBD1A}    SpSharedRecoInst Class
{E06A0DDD-E81A-4E93-8A8D-F386C3A1B670}
{E1E0A883-AB68-4C6C-9C8C-808AF2BA4CBA}
{E1E8F15E-8BEC-45DF-83BF-50FF84D0CAB5}
{E58FA315-E206-4CA4-81CE-F34E18E672C9}
{E5B2CB7A-FD35-4D4B-A147-176FEB42244B}
{E7B6AEE0-84AE-46CE-B450-DEBF58C90889}
{EB6C9433-4AAB-4B71-8B18-8F7A3812E43A}
{EE38A9FC-437F-4D03-A593-BB92AF0D153C}
{F3AEB884-58C8-40CF-AED3-E7EEFFFAA04A}
{F3D3F924-11FC-11D3-BB97-00C04F8EE6C0}    SpCFGEngine Class
{F51C7B23-6566-424C-94CF-2C4F83EE96FF}    MS TTSEngine Class
{F66A6818-F490-431B-8CA4-4CFDA287327B}    MSTTS LTS Class
{F7A465EE-13FB-409A-B878-195B420433AF}
{F7B02D8A-65DB-41CB-894D-5BBBF96C1B42}
{FBA89535-BFAB-4EF7-804C-109186BF507B}
{FD339D76-EA3E-435F-AC29-3FFCE55EB35B}
{FD51544B-8050-4C68-ABAE-3E1F7A8C01D3}
Tue Jul 14 04:54:05 2009 Z
{FCDECE00-A39D-11D0-ABE7-00AA0064D470}    ScriptoSys Class
Tue Jul 14 04:54:02 2009 Z
{0655E396-25D0-11D3-9C26-00C04F8EF87C}    SpLexicon Class
{25642426-028D-4474-977B-111BB114FE3E}    PSFactoryBuffer
{3918D75F-0ACB-41F2-B733-92AA15BCECF6}    SpObjectTokenEnum Class
{455F24E9-7396-4A16-9715-7C0FDBE3EFE3}    SpNullPhoneConverter Class
{4C6F940C-3CFE-11D2-9EE7-00C04F797396}    SpTaskManager Class
{4F414126-DFE3-4629-99EE-797978317EAD}    SpPhoneticAlphabetConverter Class
{5440837F-4BFF-4AE5-A1B1-7722ECC6332A}    AccStore Class
```

Page 47

SOFTWARE OUTPUT.txt

```
{5FB7EF7D-DFF4-468a-B6B7-2FCBD188F994}   SpMemoryStream Class
{6089A37E-EB8A-482D-BD6F-F9F46904D16D}   AccServerDocMgr Class
{6572EE16-5FE5-4331-BB6D-76A49C56E423}   AccDictionary Class
{7013943A-E2EC-11D2-A086-00C04F8EF9B5}   SpStreamFormatConverter Class
{715D9C59-4442-11D2-9605-00C04F8EE628}   SpStream Class
{8DBEF13F-1948-4AA8-8CF0-048EEBED95D8}   SpCustomStream Class
{90903716-2F42-11D3-9C26-00C04F8EF87C}   SpCompressedLexicon Class
{9185F743-1143-4C28-86B5-BFF14F20E5C8}   SpPhoneConverter Class
{947812B3-2AE1-4644-BA86-9E90DED7EC91}   SpFileStream Class
{96749373-3391-11D2-9EE3-00C04F797396}   SpResourceManager Class
{96749377-3391-11D2-9EE3-00C04F797396}   SpVoice Class
{9EF96870-E160-4792-820D-48CF0649E4EC}   SpAudioFormat Class
{A8C680EB-3D32-11D2-9EE7-00C04F797396}   SpMMAudioOut Class
{A910187F-0C7A-45AC-92CC-59EDAFB77B53}   SpObjectTokenCategory Class
{AB1890A0-E91F-11D2-BB91-00C04F8EE6C0}   SpMMAudioEnum Class
{BF426F7E-7A5E-44D6-830C-A390EA9462A3}   DocWrap Class
{C02F29F0-DFCA-4DC1-8B80-ED3216E1B5E0}   SpTtsFormatConverter Class
{C79A574C-63BE-44b9-801F-283F87F898BE}   SpWaveFormatEx Class
{C9E37C15-DF92-4727-85D6-72E5EEB6995A}   SpUncompressedLexicon Class
{D9F6EE60-58C9-458B-88E1-2F908FD7F87C}   SpDataKey Class
{E2AE5372-5D40-11D2-960E-00C04F8EE628}   SpNotifyTranslator Class
{EF411752-3736-4CB4-9C8C-8EF4CCB58EFE}   SpObjectToken Class
{FC48CC30-4F3E-4fa1-803B-AD0E196A83B1}   AccClientDocMgr Class
Tue Jul 14 04:54:01 2009 Z
{1F5EEC01-1214-4D94-80C5-4BDCD2014DDD}
{434A6274-C539-4E99-88FC-44206D942775}   AccesibilityCplAdmin Class
{483afb5d-70df-4e16-abdc-a1de4d015a3e}   AzPrincipalLocator Class
{5c2dc96f-8d51-434b-b33c-379bccae77c3}   AzBizRuleContext Class
{93CB110F-9189-4349-BD9F-392D9A4D0096}   Accessibility Control Panel
{b2bcff59-a757-4b0b-a1bc-ea69981da69e}   AzAuthorizationStore Class
{D555645E-D4F8-4c29-A827-D93C859C4F2A}   Ease of Access
{FA9342F0-B15B-473C-A746-14FCD4C4A6AA}
Tue Jul 14 04:54:00 2009 Z
{8cec58e7-07a1-11d9-b15e-000d56bfe6ee}   AP Client HxHelpPane Class
Tue Jul 14 04:53:59 2009 Z
{31b7c920-2880-11d0-8d51-00a0c908dbf1}   Korean_Default Word Breaker Resources
{369647e0-17b0-11ce-9950-00aa004bbb1f}   Neutral Word Breaker
{37c84fa0-d3db-11d0-8d51-00a0c908dbf1}   Korean_Default Stemmer Resources
{4662DAA5-D393-11D0-9A56-00C04FB68BF7}
{4662DAA6-D393-11D0-9A56-00C04FB68BF7}
{4662DAA7-D393-11D0-9A56-00C04FB68BF7}
{4662DAA8-D393-11D0-9A56-00C04FB68BF7}
{4662DAA9-D393-11D0-9A56-00C04FB68BF7}
{4662DAAA-D393-11D0-9A56-00C04FB68BF7}
{4662DAAB-D393-11D0-9A56-00C04FB68BF7}
{4662DAAC-D393-11D0-9A56-00C04FB68BF7}
{4662DAAD-D393-11D0-9A56-00C04FB68BF7}
{4662DAAE-D393-11D0-9A56-00C04FB68BF7}
{4662DAAF-D393-11D0-9A56-00C04FB68BF7}
{4662DAB0-D393-11D0-9A56-00C04FB68BF7}
{5D02926A-212E-11D0-9DF9-00A0C922E6EC}   Microsoft InfoTech IStorage System
{8cec58ae-07a1-11d9-b15e-000d56bfe6ee}   AP Client HxHelpPaneServer Class
{8FA0D5A8-DEDF-11D0-9A61-00C04FB68BF7}
{9D148290-B9C8-11D0-A4CC-0000F80149F6}   Microsoft InfoTech Protocol for IE 3.0
{9D148291-B9C8-11D0-A4CC-0000F80149F6}   Microsoft InfoTech Protocols for IE 4.0
{cca22cf4-59fe-11d1-bbff-00c04fb97fda}   Thai_Default Word Breaker Resources
{cedc01c7-59fe-11d1-bbff-00c04fb97fda}   Thai_Default Stemmer Resources
{D54EEE56-AAAB-11D0-9E1D-00A0C922E6EC}   Microsoft InfoTech IStorage for Win32
Files
Tue Jul 14 04:53:58 2009 Z
{023A36FC-E9D5-419E-824A-CDC66A116E84}   Windows Firewall with Advanced Security
{0E752416-F29E-4195-A9DD-7F0D4D5A9D71}   Windows Firewall with Advanced Security
{12a66224-5e8a-4679-8941-0b9b960bf5ea}   VistaWUWebControl Class
```

Page 48

```
                      SOFTWARE OUTPUT.txt
{12CE94A0-DEFB-11D2-B31D-00600893A857}  Chinese_Simplified Word Breaker Resources
{1CD0938D-1AC1-49DE-AA04-F2C92D4A02D1}
{2e2294a9-50d7-4fe7-a09f-e6492e185884}  rtf persistent handler
{3a64898b-20a7-4384-894b-7273c3539f2f}  MIME Filter PersistentHandler
{5645C8C1-E277-11CF-8FDA-00AA00A14F93}
{5645C8C2-E277-11CF-8FDA-00AA00A14F93}  MIME Filter
{5645C8C4-E277-11CF-8FDA-00AA00A14F93}
{73FDDC80-AEA9-101A-98A7-00AA00374959}  WordPad Document
{752438CB-E941-433F-BCB4-8B7D2329F0C8}  FwCpl LUA
{954F1760-C1BC-11D0-9692-00A0C908146E}  Chinese_Traditional Word Breaker Resources
{A4B07E49-6567-4FB8-8D39-01920E3B2357}  Virtual Factory for Windows Firewall Cpl
{ce8dbe60-d37a-4bdd-ab3a-399e69489182}
{DDECE4B2-979F-4CDB-9F58-B036FE5A510C}  Firewall Control Panel
{e2403e98-663b-4df6-b234-687789db8560}  RTF Filter
{E7E6A098-87CE-420D-91AE-413312AC8FA6}  Windows Firewall Helper Class
Tue Jul 14 04:53:55 2009 Z
{011BE22D-E453-11D1-945A-00C04FB984F9}  WSecEdit Security Manager Class
{116ABC1A-F7DB-45A7-ADDA-D5A57A08C6FF}  Workspace Setup Input Page
{165D4642-1278-4486-A3FD-439F5888FCA3}  Workspace Setup Message Page 2
{18b726bb-6fe6-4fb9-9276-ed57ce7c7cb2}  KMRDPProtocolManager  Class
{1B462D7B-72D8-4544-ACC1-D84E5B9A8A14}  MsRdpSessionManager Class
{1B6FC61A-648A-4493-A303-A1A22B543F01}  WSecEdit RSOP Security Settings Class
{1D428C79-6E2E-4351-A361-C0401A03A0BA}  PSFactoryBuffer
{228D9A81-C302-11cf-9AA4-00AA004A5691}  LDAP Provider Object
{228D9A82-C302-11cf-9AA4-00AA004A5691}  LDAP Namespace Object
{22B6E688-B3A5-44FC-B0CE-69F20653CD61}  Workspace Setup Finish Page
{241D7C96-F8BF-4F85-B01F-E2B043341A4B}  Workspaces Center
{250e91a0-0367-11cf-abc4-02608c9e7553}  WinNT Namespace Object
{274fae1f-3626-11d1-a3a4-00c04fb950dc}  ADS LDAP NameTranslate Object
{286F484D-375E-4458-A272-B138E2F80A6A}  DirectPlay8Peer Object
{2AABFCD0-1797-11D2-ABA2-00C04FB6C6FA}  WSecEdit Security Configuration Class
{2BB8B28A-58DC-449C-A89B-DAEFD0A8933D}
{2dfb3a35-6071-11d1-8c13-00c04fd8d503}  Microsoft Locality Extension
{2E8EA1E5-F406-46F5-AF10-661FD6539F28}  WSecEdit Local Security Settings Class
{3B2B6775-70B6-45AF-8DEA-A209C69559F3}  DirectPlay8LobbyClient Object
{3DECD5DD-A27B-48DC-8BAA-2682CFA265FF}  Workspace Setup Message Page
{4de7016c-5ef9-11d1-8c13-00c04fd8d503}  Microsoft User Extension
{4F1DFCA6-3AAD-48E1-8406-4BC21A501D7C}  Workspace Class
{50B6327F-AFD1-11d2-9CB9-0000F87A369E}  AD System Info Object
{59CDB915-8232-46AD-B38B-497B8B0463AD}  Workspace Setup Configure Page
{5ADF5BF6-E452-11D1-945A-00C04FB984F9}  WSecEdit Security Configuration Class
{5C0786ED-1847-11D2-ABA2-00C04FB6C6FA}  WSecEdit Security Manager Class
{5C0786EE-1847-11D2-ABA2-00C04FB6C6FA}  WSecEdit Security Settings Class
{66182EC4-AFD1-11d2-9CB9-0000F87A369E}  WinNT System Info Object
{667955AD-6B3B-43CA-B949-BC69B5BAFF7F}  DirectPlay8LobbiedApplication Object
{6A5B0C7C-5CCB-4F10-A043-B8DE007E1952}  MsRdpClientShell Class
{6D4A3650-628D-11D2-AE0F-006097B01411}  DirectPlay8 Modem Provider Object
{743B5D60-628D-11D2-AE0F-006097B01411}  DirectPlay8 Serial Provider Object
{743F1DC6-5ABA-429F-8BDF-C54D03253DC2}  DirectPlay8Client Object
{7940ACF8-60BA-4213-A7C3-F3B400EE266D}  Setup a Workspace Task Class
{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}  WSecEdit Extension Class
{8b20cd60-0f29-11cf-abc4-02608c9e7553}  WinNT Provider Object
{934A9523-A3CA-4BC5-ADA0-D6D95D979421}  DirectPlay8Address Object
{94a909a5-6f52-11d1-8c18-00c04fd8d503}  Microsoft Group Extension
{984F9804-3314-4FA4-AC8C-E688D4133C51}  Workspace Setup Confirm Settings Page
{9f37f39c-6f49-11d1-8c18-00c04fd8d503}  Microsoft PrintQueue Extension
{B43A0C1E-B63F-4691-B68F-CD807A45DA01}  MSTSWebProxy Class
{BB0D7187-3C44-11D2-BB98-3078302C2030}  CfgComp Class
{BBC035D1-E5A1-44F5-A166-E70DAED1CB02}
{CFF49D53-EE51-49F2-A807-7E3DF4EA36E3}  WSecEdit Local Security Settings Class
{D5AB5662-131D-453D-88C8-9BBA87502ADE}
Microsoft.ManagementConsole.Advanced.FrameworkSnapInFactory
{DA825E1B-6830-43D7-835D-0B5AD82956A2}  DirectPlay8Server Object
                           Page 49
```

SOFTWARE OUTPUT.txt

```
{dccc0bed-6066-11d1-8c13-00c04fd8d503}  Microsoft Organization Extension
{E4C1D9A2-CBF7-48BD-9A69-34A55E0D8941}  DirectPlay8 NAT Resolver Object
{EBFE7BA0-628D-11D2-AE0F-006097B01411}  DirectPlay8 WSock TCPIP Provider Object
{EFEA49A2-DDA5-429D-8F42-B23B92C4C347}  PSFactoryBuffer
{F0152790-D56E-4445-850E-4F3117DB740C}  Remote Sessions CPL Extension
{F975AF2C-9A51-4AF0-91EA-06038698CE38}  DirectPlay8 Diagnostics Object
{FC47060E-6153-4B34-B975-8E4121EB7F3C}  DirectPlay8 Thread Pool Object
{fd8d3a5f-6066-11d1-8c13-00c04fd8d503}  Microsoft OrganizationUnit Extension
{FE883157-CEBD-4570-B7A2-E4FE06ABE626}  WSecEdit RSOP Security Settings Class
Tue Jul 14 04:53:54 2009 Z
{01FA60A0-BBFF-11D0-8825-00A0C903B83C}  Encode CRL Distribution Points Class
{02E6EC4C-96E4-42E8-B533-336916A0087D}  PSFactoryBuffer
{19A76FE0-7494-11D0-8816-00A0C903B83C}  Encode String Array Class
{1CFC4CDA-1271-11D1-9BD4-00C04FB683FA}  Encode Alternate Name Class
{301F77B0-A470-11D0-8821-00A0C903B83C}  Encode Date Array Class
{3523c2fb-4031-44e4-9a3b-f1e94986ee7f}  Microsoft RDP Client Control - version 3
{4E0680A0-A0A2-11D0-8821-00A0C903B83C}  Encode Long Array Class
{4eb2f086-c818-447e-b32c-c51ce2b30d31}  Microsoft RDP Client Control - version 6
{4eb89ff4-7f78-4a0f-8b8d-2bf02e94e4b2}  Microsoft RDP Client Control
(redistributable) - version 6
{4EDCB26C-D24C-4e72-AF07-B576699AC0DE}  Microsoft RDP Client Control
(redistributable) - version 5
{54CE37E0-9834-41ae-9896-4DAB69DC022B}  Microsoft RDP Client Control
(redistributable) - version 5a
{54d38bf7-b1ef-4479-9674-1bd6ea465258}  Microsoft RDP Client Control - version 8
{6A6F4B83-45C5-4ca9-BDD9-0D81C12295E4}  Microsoft RDP Client Control
(redistributable) - version 4a
{6AE29350-321B-42be-BBE5-12FB5270C0DE}  Microsoft RDP Client Control - version 5
{6D6B3CD8-1278-11D1-9BD4-00C04FB683FA}  Encode Bit String Class
{7390f3d8-0439-4c05-91e3-cf5cb290c3d0}  Microsoft RDP Client Control
(redistributable) - version 7
{7584c670-2274-4efb-b00b-d6aaba6d3850}  Microsoft RDP Client Control
(redistributable) - version 4
{7cacbd7b-0d99-468f-ac33-22e495c0afe5}  Microsoft RDP Client Control - version 2
{9059f30f-4eb1-4bd2-9fdc-36f43a218f4a}  Microsoft RDP Client Control
(redistributable) - version 3
{971127BB-259F-48c2-BD75-5F97A3331551}  Microsoft RDP Client Control
(redistributable) - version 3a
{A1230201-1439-4E62-A414-190D0AC3D40E}  PSFactoryBuffer
{A1230401-67a5-4df6-a730-dce8822c80c4}
{a41a4187-5a86-4e26-b40a-856f9035d9cb}  Microsoft Terminal Services Client Control
- version 1
{a9d7038d-b5ed-472e-9c47-94bea90a5910}  Microsoft RDP Client Control
(redistributable) - version 8
{aac1009f-ab33-48f9-9a21-7f5b88426a2e}  TSRDSettings Class
{ace575fd-1fcf-4074-9401-ebab990fa9de}  Microsoft RDP Client Control - version 4
{d2ea46a7-c2bf-426b-af24-e19c44456399}  Microsoft RDP Client Control - version 7
{F9A874B6-F8A8-4D73-B5A8-AB610816828B}  Terminal Services Connection Manager Class
Tue Jul 14 04:53:53 2009 Z
{27016870-8E02-11D1-924E-00C04FBBBFB3}  MS Remote
{280A7B65-8F00-438F-989B-8EAF9E438A71}
{3449A1C8-C56C-11D0-AD72-00C04FC29863}  MSDataShape
{34AB8E82-C27E-11D1-A6C0-00C04FB94F17}
{53D6AB1D-2488-11D1-A28C-00C04FB94F17}
{69A25C12-1811-11D2-A52B-0000F803A951}
{69A25C14-1811-11D2-A52B-0000F803A951}
{93F7AA8E-CF82-4CB7-9251-48BC637A43B8}
{A1A6B99D-497F-11D1-9217-00C04FBBBFB3}  Handler Class
{E3E1D967-0829-48AC-B3AD-C5AE4CA171C4}  SQLXMLX.1
Tue Jul 14 04:53:52 2009 Z
{06210E88-01F5-11D1-B512-0080C781C384}  PSFactoryBuffer
{0C7FF16C-38E3-11d0-97AB-00C04FC2AD98}  SQLOLEDB
{0FB15084-AF41-11CE-BD2B-204C4F4F5020}  PSFactoryBuffer
```

Page 50

```
                        SOFTWARE  OUTPUT.txt
     {54AF9350-1923-11D3-9CA4-00C04F72C514}  MDACVer.Version
     {9381D8F5-0288-11d0-9501-00AA00B911A5}  RDSServer.DataFactory
     {BD96C556-65A3-11D0-983A-00C04FC29E33}  RDS.DataControl
     {BD96C556-65A3-11D0-983A-00C04FC29E36}  RDS.DataSpace
     {C0932C62-38E5-11d0-97AB-00C04FC2AD98}  SQLOLEDB Error Lookup
     {c8b522cb-5cf3-11ce-ade5-00aa0044773d}  MSDASQL
     {c8b522cc-5cf3-11ce-ade5-00aa0044773d}  MSDASQL ErrorLookup
     {c8b522cd-5cf3-11ce-ade5-00aa0044773d}  MSDASQL Enumerator
     {DFA22B8E-E68D-11d0-97E4-00C04FC2AD98}  SQLOLEDB Enumerator
     {dfc8bdc0-e378-11d0-9b30-0080c7e9fe95}  MSDAOSP
     {ef636390-f343-11d0-9477-00c04fd36226}  OLE DB Rowset Proxy
     {ef636391-f343-11d0-9477-00c04fd36226}  OLE DB Rowset Server
     {ef636392-f343-11d0-9477-00c04fd36226}  OLE DB Row Proxy
     {ef636393-f343-11d0-9477-00c04fd36226}  OLE DB Row Server
Tue Jul 14 04:53:51 2009 Z
     {016fd94e-b02a-4ab8-94c6-149fdab56b8d}  PSFactoryBuffer
     {1d16438c-54dc-404f-83a9-c041e77a32dd}  DTC Transaction Stats Control
     {1f09b058-f3fd-4a9d-a8ba-a8a05f8fe283}  DTC MMC Property-sheet extension
     {2797CF92-415A-43e6-A8F7-A5FAAB783719}  CPartitionPropPages Class
     {2C3E140B-7A0D-42d1-B2AA-D343500A90CF}  CTrkEvntListener Class
     {2f893820-7089-46cc-a6e8-c4aae45f151b}  DTC MMC Snap-in
     {410381DB-AF42-11D1-8F10-00C04FC2C17B}  COMNSView Class
     {838A77A6-14D4-439C-925F-30EE58005026}  CCOMNSScopeForExtensionSnapin Class
     {8C836AF9-FFAC-11D0-8ED4-00C04FC2C17B}  ReplicateCatalog Class
     {9305969B-F45F-47e5-A954-6EA879E874CC}  CPartitionSetPropPages Class
     {99847C33-B1B4-11D1-8F10-00C04FC2C17B}  CCOMNSScopeImpl Class
     {9cfc6d75-e648-47a8-9ea0-fb0907558952}  DTC Transaction List Control
     {a00e1768-4a9b-4d97-afc6-99d329f605f2}  CPartitionNotify Class
     {AB790AA1-CDC1-478a-9351-B2E05CFCAD09}  CPartitionContextMenu Class
     {C9BC92DF-5B9A-11D1-8F00-00C04FC2C17B}  ComponentDataImpl Class
     {D7FCB63B-5C55-11D1-8F00-00C04FC2C17B}  SnapinAboutImpl Class
     {DFFFAE4D-F0CF-46CD-9586-FE891237AB8A}  ComponentServicesExtensionSnapin Class
     {EEBD2F15-87EE-4f93-856F-6AD7E31787B3}  CPartitionSetContextMenu Class
     {FA3E1D55-16DF-446d-872E-BD04D4F39C93}  CUserPropPages Class
Tue Jul 14 04:53:50 2009 Z
     {0CF32AA1-7571-11D0-93C4-00AA00A3DDEA}  System Monitor Source Properties
     {1d27f844-3a1f-4410-85ac-14651078412d}  CompatContextMenu Class
     {513D916F-2A8E-4F51-AEAB-0CBC76FB1AF8}  LayerUIPropPage
     {7478EF61-8C46-11d1-8D99-00A0C913CAD4}  ComponentData Class
     {7478EF65-8C46-11d1-8D99-00A0C913CAD4}  ComponentData Class
     {7478EF69-8C46-11d1-8D99-00A0C913CAD4}  PerformanceAbout Class
     {74b077e8-32de-40ab-be4e-65609f575459}  Resource Monitor
     {855fec53-d2e4-4999-9e87-3414e9cf0ff4}  RunTask
     {C3E5D3D2-1A03-11CF-942D-008029004347}  System Monitor General Properties
     {C3E5D3D3-1A03-11CF-942D-008029004347}  System Monitor Graph Properties
     {C4D2D8E0-D1DD-11CE-940F-008029004347}  System Monitor Control
     {CF948561-EDE8-11CE-941E-008029004347}  System Monitor Data Properties
     {D3075F87-A7BD-4231-9F6A-60C5E07374A7}
     {E49741E9-93A8-4AB1-8E96-BF4482282E9C}  System Monitor Appearance Properties
Tue Jul 14 04:53:49 2009 Z
     {06587E71-F043-403A-BF49-CB591BA6E103}  AudioVolume Class
     {07252659-bb6b-4b79-b78b-623f6699a579}  AudioConstrictor Class
     {0E681C52-CD03-11D2-8853-0000F80883E3}
     {101193C0-0BFE-11D0-AF91-00AA00B67A42}  Display
     {1206F5F1-0569-412C-8FEC-3204630DFB70}  Credential Manager
     {129D7E40-C10D-11D0-AFB9-00AA00B67A42}  DV Muxer
     {12DD4DBB-532B-4FCE-8653-74CDB9C8FE5A}  AudioMixer Class
     {13AA3650-BB6F-11D0-AFB9-00AA00B67A42}  DV Video Encoder
     {1FE45ED3-B842-4CF2-8DF6-43E3D6D10E64}  audiokscaptureendpoint class
     {20404060-F24F-4F89-84C6-8AF80B0A17CB}  AudioKSRenderEndpoint Class
     {27c98999-2895-4829-b080-5a8b65bd3db0}  AudioRateConvertCMPT Class
     {294935CE-F637-4E7C-A41B-AB255460B862}
     {2968B3C3-CC07-40BE-B78F-094B7C310479}
                            Page 51
```

SOFTWARE OUTPUT.txt

```
{3BF043EF-A974-49B3-8322-B853CF1E5EC5}  Microsoft VolumeControlService Class
{3DC09436-7D83-4BA0-ADDC-CD47F996C5BA}  AudioMeter Class
{3fd7f233-a716-472e-8f2f-c25954f34e96}  AudioFormatConvert Class
{3FF23902-CD1F-11D2-8853-0000F80883E3}
{4150F050-BB6F-11D0-AFB9-00AA00B67A42}  Format
{41FCCC3A-1FA1-4949-953A-6EE61C46A4D1}  Microsoft.Audio.AudioClient Binder
{49c47ce0-9ba4-11d0-8212-00c04fc32c45}  SFilter Class
{49C47CE4-9BA4-11D0-8212-00C04FC32C45}  Stream Class
{49c47ce5-9ba4-11d0-8212-00c04fc32c45}  MMStream Class
{4EB31670-9FC6-11CF-AF6E-00AA00B67A42}  DV Splitter
{503739d0-4c5e-4cfd-b3ba-d881334f0df2}  VaultCredProvider
{525C410E-B007-4F15-81DD-49DF9B17139B}
{541987EE-0E02-411E-9A85-1FC6156E7F4B}  audiomatrix class
{565DCEF2-AFC5-11D2-8853-0000F80883E3}
{5BFD515E-4ABA-4483-A1C5-6651B7110AB6}  CrossProcessServerOutputEndpoint Class
{75269C13-41E1-4D0E-B8A0-9F8F22E246C9}  SystemAudioDeviceExclusive Class
{7FF0997A-1999-4286-A73C-622B8814E7EB}  ICodecAPIProxy
{8496e040-af4c-11d0-8212-00c04fc32c45}  AuStream Class
{870AF99C-171D-4f9e-AF0D-E63DF40C2BC9}
{888D5481-CABB-11D1-8505-00A0C91F9CA0}  VideoRenderCtl Class
{89115307-8248-448f-ADA0-F3F3718A9B2A}  SystemAudioDeviceShared Class
{948CFD8C-1888-4E52-8703-99610347EBB6}  AudioPump Class
{9B8C4620-2C1A-11D0-8493-00A02438AD48}  DVD Navigator
{9DBA709C-B3E1-4013-95B7-5ED33A2E8561}  CrossProcessServerInput Class
{A73BEEB2-B0B7-11D2-8853-0000F80883E3}
{ADD18BF7-AB60-4283-A580-D7544DD255D2}  AudioDeviceGraph Class
{B05DABD9-56E5-4FDC-AFA4-8A47E91F1C9C}  IVideoEncoderCodecAPIProxy
{B1B77C00-C3E4-11CF-AF79-00AA00B67A42}  DV Video Decoder
{B43C4EEC-8C32-4791-9102-508ADA5EE8E7}  IVideoEncoderProxy
{C58BD103-E87F-4B78-A0FA-7A5C95970EE2}  AudioRateConvert Class
{CD773740-B187-4974-A1D5-E0FF91372277}  CrossProcessClientOutput Class
{CF0F2F7C-F7BF-11d0-900D-00C04FD9189D}  MtStream Class
{d69e0717-dd4b-4b25-997a-da813833b8ac}  AudioLimiter Class
{E1150CE9-5BD4-4044-8FE9-98CF40137A41}  AudioProcessor Class
{e916b6b2-22bd-4afc-b337-d3d9fb27670e}  AudioCopy Class
{f2468580-af8a-11d0-8212-00c04fc32c45}  AuStream Class
{F2DDFC82-8F12-4CDD-B7DC-D4FE1425AA4D}  Sound Control Panel
{F64A6DA6-E8AF-4B7B-BCA8-847AE765D538}  CrossProcessClientInputEndpoint class
{F963C5CF-A659-4A93-9638-CAF3CD277D13}  DVD State
{FAC67227-E178-4fab-9FEA-B4E77D3DBE7D}  Video Extension Class
{FCC152B7-F372-11D0-8E00-00C04FD7C08B}  DVD Graph Builder
{FD7F2B29-24D0-4B5C-B177-592C39F9CA10}  psfactorybuffer
Tue Jul 14 04:53:48 2009 Z
{7444C717-39BF-11D1-8CD9-00C04FC29D45}  CryptPKO Class
{7444C719-39BF-11D1-8CD9-00C04FC29D45}  CryptSig Class
{B9F8AC3E-0F71-11D2-B72C-00C04FB6BD3D}  Ks IBasicAudio Interface Handler
Tue Jul 14 04:53:47 2009 Z
{148BD520-A2AB-11CE-B11F-00AA00530503}  Scheduling Agent Task Object Class
{148BD52A-A2AB-11CE-B11F-00AA00530503}  Scheduling Agent Service Class
{3c6859ce-230b-48a4-be6c-932c0c202048}  Sxs Store Class
{4729dc2b-36ff-405f-bd36-f45113adb052}  Component Based Servicing Retry Session
{75207391-23F2-4396-85F0-8FDB879ED0ED}  Component Based Servicing Session
Proxy/Stub
{752073A1-23F2-4396-85F0-8FDB879ED0ED}  Component Based Servicing Session
{8601319a-d7cf-40f3-9025-7f77125453c6}  Sxs Store Class Proxy/Stub
{8F5DF053-3013-4dd8-B5F4-88214E81C0CF}  SFP Repair Class
{90ED9FAA-A6E5-4671-8E50-1C060F8B9C47}  SFP Interface Class
{A65B8071-3BFE-4213-9A5B-491DA4461CA7}  DxDiagProvider Class
Tue Jul 14 04:53:46 2009 Z
{01575CFE-9A55-4003-A5E1-F38D1EBDCBE1}  MsCtfMonitor task handler
{05238C14-A6E1-11D0-9A84-00C04FD8DBF7}  PSFactoryBuffer
{1B1A897E-FBEE-41CF-8C48-9BF764F62B8B}  SoftKbd Class
{3318360C-1AFC-4D09-A86B-9F9CB6DCEB9C}  ClassicLangBar
```

Page 52

```
                           SOFTWARE OUTPUT.txt
   {394C052E-B830-11D0-9A86-00C04FD8DBF7}
   {4955DD33-B159-11D0-8FCF-00AA006BCC59}    CActiveIMMApp
   {50D5107A-D278-4871-8989-F4CEAAF59CFC}    CActiveIMMAppEX_Trident
   {540D8A8B-1C3F-4E32-8132-530F6A502090}    Language bar
   {5C659257-E236-11D2-8899-00104B2AFB46}    WMISnapin Class
   {5C659258-E236-11D2-8899-00104B2AFB46}    Allows configuration and control of the
Windows Management Instrumentation (WMI) service.
   {6A49950E-CE8A-4EF7-88B4-9D112366511C}    SoftKbdRegistry Class
   {93AC9CB8-27D5-4482-BFDF-68F21C7454A3}    Microsoft Shared Correction UI
   {975797FC-4E2A-11D0-B702-00C04FD8DBF7}
   {A1B9E04A-3226-11D2-883E-00104B2AFB46}    SDSnapin Description
   {AE6BE008-07FB-400D-8BEB-337A64F7051F}    TF_TransitoryExtensionUIEntry
   {B5F8FB3B-393F-4F7C-84CB-504924C2705A}    PSFactoryBuffer
   {BD95BA60-2E26-AAD1-AD99-00AA00B8E05A}    SDSnapin Class
   {C1EE01F2-B3B6-4A6A-9DDD-E988C088EC82}    CActiveIMMAppEX
   {E429B25A-E5D3-4D1F-9BE3-0C608477E3A1}    Table Driven Text Input Processor
   {F778C6B4-C08B-11D2-976C-00C04F79DB19}
   {F89E9E58-BD2F-4008-9AC2-0F816C09F4EE}    SoftKbdIMX Class
Tue Jul 14 04:53:45 2009 Z
   {0725C3CB-FEFB-11D0-99F9-00C04FC2F8EC}    WDM Event Provider
   {172BDDF8-CEEA-11D1-8B05-00600806D9B6}    Wbem Scripting Object Path
   {1EF94880-01A8-11D2-A90B-00AA00BF3363}    Microsoft NT DS Class Provider for WBEM
   {23B77E99-5C2D-482D-A795-62CA3AE5B673}    WBEM IP Route Provider
   {266C72D4-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Log File Event Consumer
Provider
   {266C72E5-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Command Line Event Consumer
Provider
   {266C72E6-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM NT Event Log Event Consumer
Provider
   {266C72E7-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Active Scripting Event
Consumer Provider
   {33831ED4-42B8-11D2-93AD-00805F853771}    Microsoft NT DS Class Associations
Provider for WBEM
   {35B78F79-B973-48C8-A045-CAEC732A35D5}    WDM HiPerf Provider
   {443C8934-90FF-48ED-BCDE-26F5C7450042}    PSFactoryBuffer
   {47DFBE54-CF76-11D3-B38F-00105A1F473A}    WBEM Scripting DateTime
   {54B50739-686F-45EB-9DFF-D6A9A0FAA9AF}    PSFactoryBuffer
   {5791BC26-CE9C-11D1-97BF-0000F81E849C}    WBEM Scripting Object Path
   {5CE34C0D-0DC9-4C1F-897C-DAA1B78CEE7C}    PSFactoryBuffer
   {6515834D-6125-4878-A3A3-6B0A73B809A2}    Win32_JobObjectLimitInfo Component
   {659CDEAD-489E-11D9-A9CD-000D56965251}    PSFactoryBuffer
   {659CDEAE-489E-11D9-A9CD-000D56965251}    psfactorybuffer
   {6D7A4B0E-66D5-4AC3-A7ED-0189E8CF5E77}    WBEM IP Route Event Provider
   {72967901-68EC-11D0-B729-00AA0062CBB7}    WBEM Registry Property Provider
   {72967903-68EC-11D0-B729-00AA0062CBB7}    WBEM PerfMon Property Provider
   {734AC5AE-68E1-4FB5-B8DA-1D92F7FC6661}    WBEM Ping Provider
   {75718C9A-F029-11D1-A1AC-00C04FB6C223}    WBEM Scripting Sink
   {76A64158-CB41-11D1-8B02-00600806D9B6}    WBEM Scripting Locator
   {7FB1D98A-F895-4761-8DC2-774969C84D10}    Win32_JobObject Provider Component
   {9877D8A7-FDA1-43F9-AEEA-F90747EA66B0}    KernelTraceProvider Class
   {9a2584c3-f7d2-457a-9a5e-22b67bffc7d2}    psfactorybuffer
   {9AED384E-CE8B-11D1-8B05-00600806D9B6}    WBEM Scripting Named Value Collection
   {AA527A40-4D9A-11D2-93AD-00805F853771}    Microsoft NT DS Instance Provider for WBEM
   {AA70DDF4-E11C-11D1-ABB0-00C04FD9159E}    Microsoft WBEM View Provider
   {AB40A5C1-804B-40BD-9DFE-A640691C6956}    Win32_JobObjectSecLimitInfo Component
   {BE0A9830-2B8B-11D1-A949-0060181EBBAD}    WMI MSI Provider
   {C0AA9D93-2EF5-47FB-960C-F90FC644B48E}    Win32_JobObjectIOAccountingInfo Component
   {C2FEEEAC-CFCD-11D1-8B05-00600806D9B6}    Wbem Scripting Last Error
   {C4819C8D-9AB8-4B2F-B8AE-C77DABF553D5}    Microsoft WBEM Current Time Provider
   {C7A3A54B-0250-11D3-9CD1-00105A1F4801}    Microsoft WBEM SMTP Event Consumer
Provider
   {D269BF5C-D9C1-11D3-B38F-00105A1F473A}    WBEM Scripting Refresher
   {D2D588B5-D081-11D0-99E0-00C04FC2F8EC}    WDM Instance Provider
                                Page 53
```

SOFTWARE OUTPUT.txt

```
{ef7e0655-7888-4960-b0e5-730846e03492}  psfactorybuffer
{F00B4404-F8F1-11CE-A5B6-00AA00680C3F}  WBEM PerfMon Instance Provider
{f1bd1079-9f01-4bdc-8036-f09b70095066}  psfactorybuffer
{F55C5B4C-517D-11D1-AB57-00C04FD9159E}  Microsoft WBEM NT Eventlog Event Provider
{FA77A74E-E109-11D0-AD6E-00C04FD8FDFF}  WBEM Registry Event Provider
{FD4F53E0-65DC-11D1-AB64-00C04FD9159E}  Microsoft WBEM NT Eventlog Instance
Provider
{FE9AF5C0-D3B6-11CE-A5B6-00AA00680C3F}  WBEM Registry Instance Provider
Tue Jul 14 04:53:43 2009 Z
{066D2323-D35A-4C15-AE22-F88F136C1613}  KeystrokeGenerator Class
{0A56CD6C-B45A-4A6C-A88C-3F42AC7BCED4}  KeyStrokeMonitor Class
{220A0D48-03A8-4F7B-8408-4EB506EF68D9}  PSFactoryBuffer
{632B0530-3CBF-44F4-BFDC-750A80D4B00A}  StateController Class
{634F8410-E924-46B8-A1B5-E8B08E8B8750}  PSFactoryBuffer
{68904ac7-1801-47f8-af3a-dac14848fd75}  PSFactoryBuffer
{6A514DB9-3EC1-4F36-9F95-BC0B00152D0B}  DefinitionParser Class
{6af6b181-3a90-4fac-9655-b34041d46b8f}  PSFactoryBuffer
{884CFF4F-0BB0-4CAA-83BD-4FB9ECE938FA}  DefinitionLoader Class
{BFC7DC7B-8F11-4A40-8DB2-207302E2D61B}  PSFactoryBuffer
{E13B9A7F-EC39-4E7F-9970-12F348C89FD0}  PSFactoryBuffer
{E787250A-F3B3-4e8d-A300-F58FB129B709}  PSFactoryBuffer
{E800E945-780D-48D3-89E7-D822EA18F0A2}  PSFactoryBuffer
{F3252D7B-E51D-4B14-AA5E-8E3D4315F73C}  PSFactoryBuffer
Tue Jul 14 04:53:38 2009 Z
CLSID   {0000031A-0000-0000-C000-000000000046}
{0000002F-0000-0000-C000-000000000046}  CLSID_RecordInfo
{00000300-0000-0000-C000-000000000046}  StdOleLink
{00000301-A8F2-4877-BA0A-FD2B6645FB94}  PSFactoryBuffer
{00000303-0000-0000-C000-000000000046}  FileMoniker
{00000304-0000-0000-C000-000000000046}  ItemMoniker
{00000305-0000-0000-C000-000000000046}  AntiMoniker
{00000306-0000-0000-C000-000000000046}  PointerMoniker
{00000308-0000-0000-C000-000000000046}  PackagerMoniker
{00000309-0000-0000-C000-000000000046}  CompositeMoniker
{0000030B-0000-0000-C000-000000000046}  DfMarshal
{00000315-0000-0000-C000-000000000046}  Picture (Metafile)
{00000316-0000-0000-C000-000000000046}  Picture (Device Independent Bitmap)
{00000319-0000-0000-C000-000000000046}  Picture (Enhanced Metafile)
{0000031A-0000-0000-C000-000000000046}  ClassMoniker
{0000031D-0000-0000-C000-000000000046}  DCOMAccessControl
{00000320-0000-0000-C000-000000000046}  PSFactoryBuffer
{00000327-0000-0000-C000-000000000046}  objref
{0000032E-0000-0000-C000-000000000046}  PipePSFactory
{00000507-0000-0010-8000-00AA006D2EA4}  ADODB.Command
{0000050B-0000-0010-8000-00AA006D2EA4}  ADODB.Parameter
{00000514-0000-0010-8000-00AA006D2EA4}  ADODB.Connection
{0000051A-0000-0010-8000-00AA006D2EA4}  ADO 6.0
{00000535-0000-0010-8000-00AA006D2EA4}  ADODB.Recordset
{00000541-0000-0010-8000-00AA006D2EA4}  ADODB.Error
{00000542-0000-0010-8000-00AA006D2EA4}  ADODB Error Lookup Service
{00000560-0000-0010-8000-00AA006D2EA4}  ADODB.Record
{00000566-0000-0010-8000-00AA006D2EA4}  ADODB.Stream
{00000602-0000-0010-8000-00AA006D2EA4}  ADOX.Catalog.6.0
{00000609-0000-0010-8000-00AA006D2EA4}  ADOX.Table.6.0
{00000615-0000-0010-8000-00AA006D2EA4}  ADOX.Group.6.0
{00000618-0000-0010-8000-00AA006D2EA4}  ADOX.User.6.0
{0000061B-0000-0010-8000-00AA006D2EA4}  ADOX.Column.6.0
{0000061E-0000-0010-8000-00AA006D2EA4}  ADOX.Index.6.0
{00000621-0000-0010-8000-00AA006D2EA4}  ADOX.Key.6.0
{00020000-0000-0000-C000-000000000046}  Microsoft AVI Files
{00020001-0000-0000-C000-000000000046}  AVI Compressed Stream
{00020003-0000-0000-C000-000000000046}  Microsoft Wave File
{0002000D-0000-0000-C000-000000000046}  IAVIStream & IAVIFile Proxy
```

Page 54

```
                           SOFTWARE OUTPUT.txt
{0002000F-0000-0000-C000-000000000046}  ACM Compressed Audio Stream
{00020420-0000-0000-C000-000000000046}  PSDispatch
{00020421-0000-0000-C000-000000000046}  PSEnumVariant
{00020422-0000-0000-C000-000000000046}  PSTypeInfo
{00020423-0000-0000-C000-000000000046}  PSTypeLib
{00020424-0000-0000-C000-000000000046}  PSOAInterface
{00020425-0000-0000-C000-000000000046}  PSTypeComp
{00020810-0000-0000-C000-000000000046}
{00020811-0000-0000-C000-000000000046}
{00020900-0000-0000-C000-000000000046}
{00020D75-0000-0000-C000-000000000046}
{00021400-0000-0000-C000-000000000046}  Desktop
{00021401-0000-0000-C000-000000000046}  Shortcut
{0002E005-0000-0000-C000-000000000046}  Component Categories Manager
{0002E006-0000-0000-C000-000000000046}  Component Categories Manager With Class
Store
{000C101C-0000-0000-C000-000000000046}  Msi install server
{000C101D-0000-0000-C000-000000000046}  Microsoft Windows Installer Message RPC
{000C103E-0000-0000-C000-000000000046}  PSFactoryBuffer
{000C1090-0000-0000-C000-000000000046}  Microsoft Windows Installer
{000C1094-0000-0000-C000-000000000046}
{0010668C-0801-4DA6-A4A4-826522B6D28F}
{00108226-EE41-44A2-9E9C-4BE4D5B1D2CD}
{0010890e-8789-413c-adbc-48f5b511b3af}  User Notification
{00393519-3A67-4507-A2B8-85146167ACA7}  WPD Association LUA Virtual Factory
{003e0278-eca8-4bb8-a256-3689ca1c2600}  Published Items Shell Service Object
{00597829-82CE-44d4-8B0B-40BE695973B5}  WMPDMCServersManager Class
{006E61DF-1A43-4F2C-B26F-780BAEA3A92D}
{0086c339-9c0e-4c09-9a2f-ff3d19a44a18}  PSFactoryBuffer
{009f3b45-8a6b-4360-b997-b2a009a16402}  XWizard Factory Generated Class (HomeGroup
Update Passkey/Merge Hook Page)
{00BB2763-6A77-11D0-A535-00C04FD7D062}  Microsoft AutoComplete
{00BB2764-6A77-11D0-A535-00C04FD7D062}  Microsoft History AutoComplete List
{00BB2765-6A77-11D0-A535-00C04FD7D062}  Microsoft Multiple AutoComplete List
Container
{00da2f99-f2a6-40c2-b770-a920f8e44abc}  Staging ShellFolder for CD Burning
{00eebf57-477d-4084-9921-7ab3c2c9459d}  CD Burn Merged Folder
{00f20eb5-8fd6-4d9d-b75e-36801766c8f1}  PhotoAcqDropTarget
{00f210a1-62f0-438b-9f7e-9618d72a1831}  PhotoAcquireOptionsDialog
{00f24ca0-748f-4e8a-894f-0e0357c6799f}  PhotoProgressDialog
{00f26e02-e9f2-4a9f-9fdd-5a962fb26a98}  PhotoAcquire
{00f29a34-b8a1-482c-bcf8-3ac7b0fe8f62}  PhotoAcqDeviceSelectionDlg
{00f2b433-44e4-4d88-b2b0-2698a0a91dba}  PhotoAcqHWEventHandler
{00F2CE1E-935E-4248-892C-130F32C45CB4}  PSFactoryBuffer
{0102563D-F16D-434d-82A2-37968BD3E31E}  RNWF Extensible Helper Class
{011B3619-FE63-4814-8A84-15A194CE9CE3}  WebDVD Device Segment
{0131BE10-2001-4C5F-A9B0-CC88FAB64CE8}
{0142e4d0-fb7a-11dc-ba4a-000ffe7ab428}  Biometrics
{0142e4d1-fb7a-11dc-ba4a-000ffe7ab428}  Virtual Factory for Biometrics
{0142e4d2-fb7a-11dc-ba4a-000ffe7ab428}
{0142e4d3-fb7a-11dc-ba4a-000ffe7ab428}
{01458CF0-A1A2-11D1-8F85-00600895E7D5}  Interface Proxy Stub
{0149EEDF-D08F-4142-8D73-D23903D21E90}  XDS Feature Segment
{01822ABA-23F0-4506-9BBC-680F5D6D606C}  CLSID_ContactUserAccountChangeCallback
{01A3BF5C-CC93-4C12-A4C3-09B0BBE7F63F}
{01afc156-f2eb-4c1c-a722-8550417d396f}  Action Center PSFactory
{01CBCF66-A9CA-4449-84DE-7F321232BBC7}  html persistent handler for mapi email
{01E04581-4EEE-11d0-BFE9-00AA005B4383}  &Address
{01F36CE2-0907-4d8b-979D-F151BE91C883}  CFrameRateConvertDmo
{021003e9-aac0-4975-979f-14b5d4e717f8}  LocalCopyHelper
{02805F1E-D5AA-415B-82C5-61C033A988A6}
{02df6db6-9405-4812-b3f6-500e8615b7af}  Registry Data Driven Command
{03012959-F4F6-44D7-9D09-DAA087A9DB57}
                              Page 55
```

```
                          SOFTWARE OUTPUT.txt
   {03022430-ABC4-11D0-BDE2-00AA001A1953}  PSFactoryBuffer
   {031E4825-7B94-4dc3-B131-E946B44C8DD5}  UsersLibraries
   {031EE060-67BC-460d-8847-E4A7C5E45A27}  Windows Media Player Rich Preview Handler
   {0344ec28-5339-4124-a186-2e8eef168785}  MFSourceFilter
   {0369B4E5-45B6-11D3-B650-00C04F79498E}  BDA Tuning Model Channel Tune Request
   {0369B4E6-45B6-11D3-B650-00C04F79498E}  BDA Tuning Model ATSC Channel Tune Request
   {036A9790-C153-11D2-9EF7-006008039E37}  Audio Mixer
   {03837511-098B-11D8-9414-505054503030}  TraceDataProviderCollection
   {03837513-098B-11D8-9414-505054503030}  TraceDataProvider
   {0383751C-098B-11D8-9414-505054503030}  TraceSession
   {03837521-098B-11D8-9414-505054503030}  DataCollectorSet
   {03837525-098B-11D8-9414-505054503030}  DataCollectorSetCollection
   {03837526-098B-11D8-9414-505054503030}  LegacyDataCollectorSet
   {03837527-098B-11D8-9414-505054503030}  LegacyDataCollectorSetCollection
   {03837528-098B-11D8-9414-505054503030}  LegacyTraceSession
   {03837529-098B-11D8-9414-505054503030}  LegacyTraceSessionCollection
   {03837530-098B-11D8-9414-505054503030}  TraceSessionCollection
   {03837531-098B-11D8-9414-505054503030}  ServerDataCollectorSet
   {03837532-098B-11D8-9414-505054503030}  ServerDataCollectorSetCollection
   {03837538-098B-11D8-9414-505054503030}  BootTraceSession
   {03837539-098B-11D8-9414-505054503030}  BootTraceSessionCollection
   {03837546-098B-11D8-9414-505054503030}  ServerDataCollectorSet
   {03837547-098B-11D8-9414-505054503030}  SystemDataCollectorSetCollection
   {03A0E2CD-23A9-45ed-968F-6FDA22B2285E}  New Network Category Custom Page
   {03C036F1-A186-11D0-824A-00AA005B4383}  Microsoft Shell Folder AutoComplete List
   {03C06416-D127-407A-AB4C-FDD279ABBE5D}  BDA Tuning Model Digital Cable Locator
   {03ca98d6-ff5d-49b8-abc6-03dd84127020}  Background Intelligent Transfer Control
Class 2.5
   {03e15b2e-cca6-451c-8fb0-1e2ee37a27dd}  CTapiLuaLib Class
   {0429EC6E-1144-4bed-B88B-2FB9899A4A3D}  Custom Composition Segment from Data
Services to XDS
   {042dc17c-023f-43df-a3ec-982b4dc78a64}  Schema Migration Plugin
   {04731B67-D933-450a-90E6-4ACD2E9408FE}  CLSID_SearchFolder
   {04788120-12C2-498D-83C1-A7D92E677AC6}  WBEM Framework Instance Provider CIMA
   {0482DDE0-7817-11CF-8A03-00AA006ECB65}  KsDataTypeHandlerAnalogVideo
   {0482E074-C5B7-101A-82E0-08002B36A333}
   {04a1e553-fe36-4fde-865e-344194e69424}  Microsoft InkPicture Control
   {04A578B2-E778-422A-A805-B3EE54D90BD9}  PSFactoryBuffer
   {04B55BC3-33DE-4d79-94EC-830CDF96CC82}  WMPlayer ContentPropPage Class
   {04FBCBF4-DC23-3CEC-9025-9D4093C26733}
   {0520af9e-e3da-4b32-8be8-0f3e475bfc5f}  Device Center Print Status Extension
   {05300401-BCBC-11d0-85E3-00C04FD85AB4}  MHTML Asynchronous Pluggable Protocol
Handler
   {05589F80-C356-11CE-BF01-00AA0055595A}  KsDataTypeHandlerVideo
   {05589FA1-C356-11CE-BF01-00AA0055595A}  ActiveMovieControl Object
   {05589FAF-C356-11CE-BF01-00AA0055595A}  Audio Renderer Property Page
   {055CB2D7-2969-45CD-914B-76890722F112}  BDA Tuning Model MPEG2 Component Class
(Broadcast Substream)
   {056440FD-8568-48e7-A632-72157243B55B}  Explorer Navigation Bar
   {05DF8D13-C355-47f4-A11E-851B338CEFB8}  CQueryAllWinSAT Class
   {05F3561D-0358-4687-8ACD-A34D24C488DF}  Health Center Control Panel
   {060AF76C-68DD-11D0-8FC1-00C04FD9189D}  Seeking
   {06290BD0-48AA-11D2-8432-006008C3FBFC}  Object under which scriptlets may be
created
   {06290BD1-48AA-11D2-8432-006008C3FBFC}  Constructor that allows hosts better
control creating scriptlets
   {06290BD2-48AA-11D2-8432-006008C3FBFC}  Factory bindable using IPersistMoniker
   {06290BD3-48AA-11D2-8432-006008C3FBFC}  Moniker to a Windows Script Component
   {06290BD4-48AA-11D2-8432-006008C3FBFC}  Object for encoding scriptlets
   {06290BD5-48AA-11D2-8432-006008C3FBFC}  Object for constructing type libraries for
scriptlets
   {06290BD8-48AA-11D2-8432-006008C3FBFC}  Constructor for Scriptlet Automation
Handler
```

Page 56

SOFTWARE OUTPUT.txt

```
{06290BD9-48AA-11D2-8432-006008C3FBFC}  Constructor for Scriptlet Event Handler
{06290BDA-48AA-11D2-8432-006008C3FBFC}  Constructor for Scriptlet ASP Handler
{06290BDB-48AA-11D2-8432-006008C3FBFC}  Constructor for Scriptlet Behavior Handler
{063B79F5-7539-11D2-9773-00A0C9B4D50C}  Microsoft COM+ Services Meta Data
{063B79F6-7539-11D2-9773-00A0C9B4D50C}  Microsoft COM+ Services Meta Data
{06622D85-6856-4460-8DE1-A81921B41C4B}  CopenControlPanel
{067B4B81-B1EC-489f-B111-940EBDC44EBE}  WMDM CE Device Service Provider
{06A03425-C9EB-11d2-8CAA-0080C739E3E0}  Help Collection Wrapper Class
{06B32AEE-77DA-484B-973B-5D64F47201B0}  VMR Mixer
{06C792F8-6212-4F39-BF70-E8C0AC965C23}  User Account Control Settings
{06CCA63E-9941-441B-B004-39F999ADA412}  MMEndpointManager class
{06EEE695-542D-46F6-AEAB-FA2F1B2102D3}  GameCleanupHandler Class
{0700F42F-EEE3-443a-9899-166F16286796}  HomeGroup Network
{07398dcf-2e0b-4ece-99dd-56b262db948b}  Search Protocol URL Generator
{078759d3-423b-48ad-ab6a-5638c2884dbe}  Shell Undo Parent Unit
{079AA557-4A18-424A-8EEE-E39F0A8D41B9}  SAX XML Reader
{07A774A0-6047-11D1-BA20-006097D2898E}  Logagent Class
{07AA0886-CC8D-4e19-A410-1C75AF686E62}  Onex  PLAP Credential Provider
{07B65360-C445-11CE-AFDE-00AA006C14F4}  MIDI Renderer
{07D26616-6136-11D1-8C9C-00C04FC3261D}
{080d0d78-f421-11d0-a36e-00c04fb950dc}  ADs LDAP Pathname Descriptor Object
{08244EE6-92F0-47f2-9FC9-929BAA2E7235}  Sharing Overlay (Private)
{083863F1-70DE-11D0-BD40-00A0C911CE86}  ActiveMovie Filter Class Manager
{08a99e2f-6d6d-4b80-af5a-baf2bcbe4cb9}  PropVariantCollection Class
{08d5bfbf-fbca-4322-9f70-ca9f66f8ed6a}  CommonLayoutModifier
{09017262-fdb4-4ff2-9013-26332c926ee7}  Csc Sync
{09144FD6-BB29-11DB-96F1-005056C00008}  PBDA DTFilter
{093FF999-1EA0-4079-9525-9614C3504B74}  Windows Script Host Network Object
{09474572-B2FB-11D1-A1A1-0000F875B132}  MMCListPadInfo class
{0955AC62-BF2E-4CBA-A2B9-A63F772D46CF}  BDA Tuning Model MPEG2 Tune Request
{0977EEC5-10F7-44AE-A7FA-D4824EBA5C74}  PrintersCacheManager Class
{09799AFB-AD67-11d1-ABCD-00C04FC30936}  Open With Context Menu Handler
{098f2470-bae0-11cd-b579-08002b30bfeb}  Null persistent handler
{0997898B-0713-11d2-A4AA-00C04F8EEB3E}  Common Places FS Folder
{09a28848-0e97-4cef-b950-cea037161155}  Remove Properties Drop Target
{09C20568-F30C-489B-AE9C-4930AD7F165F}  PSFactoryBuffer
{09DBBC77-588F-4517-A485-74A29759F54C}  PSFactoryBuffer
{0A16D195-6F47-4964-9287-9F4BAB6D9827}  PSFactoryBuffer
{0A29F9BD-86B3-4384-B25D-EF1FFE020266}  WSD Scan Proxy
{0A522732-A626-11D0-8D60-00C04FD6202B}  CLSID_CExchImport
{0A886F29-465A-4aea-8B8E-BE926BFAE83E}  EapQecMessenger
{0A88C858-7D0C-4549-9499-7DB05F0CB0BF}  Share Home Group
{0A9AE910-85C0-11D0-BD42-00A0C911CE86}  AVI mux Property Page1
{0AA02E8D-F851-4CB0-9F64-BBA9BE7A983D}  AlchemyVis Class
{0AE89F03-C538-4471-9B12-A8E8EF246A0D}  PSFactoryBuffer
{0af10cec-2ecd-4b92-9581-34f6ae0637f3}  PortableDeviceManager Class
{0af96ede-aebf-41ed-a1c8-cf7a685505b6}  Library Folder Context Menu
{0AFACED1-E828-11D1-9187-B532F1E9575D}  Folder Shortcut
{0AFCCBA6-BF90-4A4E-8482-0AC960981F5B}
{0B124F8F-91F0-11D1-B8B5-006008059382}  Installed Apps Enumerator
{0b2feecb-1577-4fa6-9a29-bd9022ebcf90}  CPPTPDiagHelper Object
{0B3FFB92-0919-4934-9D5B-619C719D0202}  Broadcast Event Service
{0B5A7836-4C16-4560-90B2-0F5DAF6D6D1B}  FormHost Class
{0b91a74b-ad7c-4a9d-b563-29eef9167172}  WpdSerializer Class
{0BA2A2AC-A4D5-38CB-AD03-A0D5B6EC4646}
{0BE35200-8F91-11CE-9DE3-00AA004BB851}  Font Property Page
{0BE35201-8F91-11CE-9DE3-00AA004BB851}  Color Property Page
{0BE35202-8F91-11CE-9DE3-00AA004BB851}  Picture Property Page
{0BE35203-8F91-11CE-9DE3-00AA004BB851}  Standard Font
{0BE35204-8F91-11CE-9DE3-00AA004BB851}  Standard Picture
{0BFCF7B7-E7B6-433a-B205-2904FCF040DD}  New Shortcut Wizard Modal
{0c15d503-d017-47ce-9016-7b3f978721cc}  PortableDeviceValues Class
{0C39A5CF-1A7A-40C8-BA74-8900E6DF5FCD}
```

Page 57

SOFTWARE OUTPUT.txt

```
{0C3B05FB-3498-40C3-9C03-4B22D735550C}  RasDlg LUA
{0C5672F9-3EDC-4b24-95B5-A6C54C0B79AD}  Rational Class
{0C776A5A-FC42-4870-8D65-D62ADD9184FF}  Magic USB Cable Class ID
{0cbb5030-f2b2-4b38-8cbc-895cec57db03}  Create 802.11 Ad hoc Task Class
{0cbb5031-f2b2-4b38-8cbc-895cec57db03}  Adhoc Create Adapter Selection Page Class
{0cbb5032-f2b2-4b38-8cbc-895cec57db03}  Adhoc Create Setup Page Class
{0cbb5034-f2b2-4b38-8cbc-895cec57db03}  Adhoc Create Status Page Class
{0cbb5035-f2b2-4b38-8cbc-895cec57db03}  Adhoc Create Finish Page Class
{0cbb5036-f2b2-4b38-8cbc-895cec57db03}  Adhoc Ics Option Page Class
{0cbb5037-f2b2-4b38-8cbc-895cec57db03}  Adhoc Ics Status Page Class
{0cbb5038-f2b2-4b38-8cbc-895cec57db03}  Adhoc Error Report Page Class
{0cbb503a-f2b2-4b38-8cbc-895cec57db03}  Adhoc Ics Finish Page Class
{0CE7A4A6-03E8-4A60-9D15-282EF32EE7DA}
{0CF774D0-F077-11D1-B1BC-00C04F86C324}  HTML Host Encode Object
{0CF774D1-F077-11D1-B1BC-00C04F86C324}  ASP Host Encode Object
{0CFDD070-581A-11D2-9EE6-006008039E37}  Generate Black Video
{0D0E47ED-7220-411f-8F81-1118095DA5E7}  Publication Services Change Data
{0D41EBA2-17EA-4B0D-9172-DBD2AE0CC97A}  SrDrvWuHelper Class
{0D43FE01-F093-11CF-8940-00A0C9054228}  FileSystem Object
{0D45D530-764B-11d0-A1CA-00AA00C16E65}
{0D6417E3-866C-4959-9816-4BF5B85CDAD7}  MsasrUI Class
{0d81ea0d-13bf-44b2-af1c-fcdf6be7927c}  Microsoft DocProp Custom Draw Progress
Control
{0da7bfdf-c0a0-44eb-be82-b7a82c4721de}  ARP CBS Uninstaller Proxy
{0DAD2FDD-5FD7-11D3-8F50-00C04F7971E2}  Microsoft ATSC Network Provider
{0DED49D5-A8B7-4D5D-97A1-12B0C195874D}  IBDA_PinControl
{0DF44EAA-FF21-4412-828E-260A8728E7F1}  Taskbar and Start Menu
{0E2988ED-1DCB-44D0-B9E0-C3AE1D25BE8A}  WlanDlg Suppress Autoplay Class
{0E5AAE11-A475-4c5b-AB00-C66DE400274E}  Shell File System Folder
{0E5CBF21-D15F-11D0-8301-00AA005B4383}  &Links
{0e6daa63-dd4e-47ce-bf9d-fdb72ece4a0d}  Device Center Print Context Menu Extension
{0EEA25CC-4362-4a12-850B-86EE61B0D3EB}  Microsoft DocProp Inplace Droplist Combo
Control
{0ef801bb-24e7-4059-aeb0-d8727eeaf04c}  Mobile Broadband Auto Connect Settings
Page Class
{0F424AB8-3D71-3F74-B230-EFB0144788ED}
{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  TaskScheduler class
{0fb40f0d-1021-4022-8da0-aab0588dfc8b}  UPnPAutomationProxy
{0FC988D4-C935-4b97-A973-46282EA175C8}  PSFactoryBuffer
{101A8FB9-F1B9-11d1-9A56-00C04FA309D4}  CLSID_MessageStore
{104846ab-42b1-4e38-a80d-136f78c3f258}  Browser Progress Aggregator
{10E2414A-EC59-49D2-BC51-5ADD2C36FEBC}  PSFactoryBuffer
{10FEF81C-0DAA-4af0-B714-1F1689C08C8C}  DXVA Allocator
{1108BE51-F58A-4CDA-BB99-7A0227D11D5E}  Microsoft WBEM _IWmiCallSec Call Security
Factory
{11103421-354C-4CCA-A7A3-1AFF9A5B6701}  MP3 ACM Wrapper MFT
{1138506a-b949-46a7-b6c0-ee26499fdeaf}  WUAppElevator class
{114F5598-0B22-40A0-86A1-C83EA495ADBD}
{116F8D13-101E-4fa5-84D4-FF8279381935}  CompoundCondition Class
{11993195-1244-4840-AB44-480975C4FFE4}  CFileIo
{11d162b6-1cea-4b4a-8037-2518ecd6554b}  CLSID_FTItemContainer
{11dbb47c-a525-400b-9e80-a54615a090c0}  CLSID_ExecuteFolder
{1202DB60-1DAC-42C5-AED5-1ABDD432248E}  Sync Center Client
{120CED89-3BF4-4173-A132-3CB406CF3231}  DirectSoundParamEqDMO
{122EC645-CD7E-44D8-B186-2C8C20C3B50F}
{12367cf8-6222-4b34-8ca8-3ce703999e28}  Share Command Execution
{12426E70-50E2-3129-B617-E252B36ECE89}
{1249B20C-5DD0-44FE-B0B3-8F92C8E6D080}
{12518493-00B2-11d2-9FA5-9E3420524153}  Mounted Volume
{1277B60F-34D5-48D1-B7BB-59BCA9BC71A8}  Microsoft MPEG-2 Multiplexer Encoder
Property Page
{1299CF18-C4F5-4B6A-BB0F-2299F0398E27}  PSFactoryBuffer
{12C21EA7-2EB8-4B55-9249-AC243DA8C666}  Virtual Factory for DiagCpl
```

Page 58

SOFTWARE OUTPUT.txt

```
{12D51199-0DB5-46FE-A120-47A3D7D937CC}   DVD: Pluggable Protocol
{12DA6D0B-021F-4d79-8794-64145F503CA5}   EAP Quarantine Enforcement Client Callback
Component
{12fc5e89-5446-4a7c-ba46-207a29e2945d}   HomeGroup Confirm Page
{1334e551-b2db-429b-a94a-7d6a226ffcbf}
{13482EC3-06A3-4bb3-84A9-193302B8DD54}
{13639463-00DB-4646-803D-528026140D88}   UpdateCollection Class
{13709620-C279-11CE-A49E-444553540000}   Shell Automation Service
{1372A97E-2034-41ee-A6C1-1B68FAFA75A1}   CLSID_ICommunityTransport
{137f5ec6-cf6b-482f-acea-c687dfbd199d}   Microsoft Input Personalization Plug-in
{139D8403-E74F-41d2-B103-8790C5C7A517}
{13a4bbe8-6527-40cb-a996-1602829541ef}   Frame Automation Object
{13B37A2A-546B-47BF-BBCA-8AC97F1EBDCB}   CMpeg2DataControl
{13D3C4B8-B179-4ebb-BF62-F704173E7448}   CLSID_ContactReadingPane
{13DE4A42-8D21-4C8E-BF9C-8F69CB068FCA}   E-Ink
{14010e02-bbbd-41f0-88e3-eda371216584}   CLSID_SearchFolderItemFactory
{14074e0b-7216-4862-96e6-53cada442a56}   Library Icon Extract Extension
{1438E821-B6D2-11D0-8D86-00C04FD6202B}   CLSID_ApprenticeAcctMgr
{1443904b-34e4-40f6-b30f-6beb81267b80}   cicero sapi layer speech ui server
{14795a8f-78f3-47bd-acb6-e767414fe293}   Shell Apply Properties Undo Unit
{147A9C5D-36F4-4e3e-BD47-F5F207425085}   HomeGroup Printing Listener Class
{14ce31dc-abc2-484c-b061-cf3416aed8ff}   Authentication UI Shutdown Choices
{14D4CBD9-7490-4F25-BAA6-1C5E22F6B1E3}   PimcManager Class
{14d7a407-396b-44b3-be85-5199a0f0f80a}   Media Foundation DShow Source Resolver
{14DD9A1C-7CFF-41be-B1B9-BA1AC6ECB571}   MF AudCap Source Plug-in
{1510FB87-5676-40B9-A227-5D0B66866F81}   PSFactoryBuffer
{1531d583-8375-4d3f-b5fb-d23bbd169f22}   Windows TXT Previewer
{15756be1-a4ad-449c-b576-df3df0e068d3}   Microsoft DocProp Hyperlink Control
{15b0bb4c-0f7d-11D1-b21f-00C04Fb9473f}
{15D6504A-5494-499C-886C-973C9E53B9F1}   BDA Tuning Model DVB Tune Request
{15eae92e-f17a-4431-9f28-805e482dafd4}   Install New Programs
{15FD01A3-6E5D-4ECD-9EBD-1813CB3887A1}   PSFactoryBuffer
{163FDC20-2ABC-11d0-88F0-00A024AB2DBB}
{1643E180-90F5-11CE-97D5-00AA0055595A}   Color Space Converter
{1649b154-c794-497a-9b03-f3f0121302f3}   PortableDeviceServiceFTM Class
{1649d1cf-deaf-4a68-abe8-5c9f68572fd1}   ExecuteAssociation
{16671E5F-0CE6-4CC4-9768-E89FE5018ADE}
{167c0a56-c490-4623-9225-8ffdc546e56c}   Top view restore default command
invocation
{1698790a-e2b4-11d0-b0b1-00c04fd8dca6}
{169A0691-8DF9-11d1-A1C4-00C04FD75D13}   In-pane search
{16C2C29D-0E5F-45f3-A445-03E03F587B7D}   .group shell context menu
{16CA4E03-FE69-4705-BD41-5B7DFC0C95F3}   PSFactoryBuffer
{1767B93A-B021-44EA-920F-863C11F4F768}
{176961ec-fbfb-4288-b418-c80c86947481}   CVPNDiagHelper Object
{176D323D-E591-4535-9A09-26F698E5AC5D}   UserLexiconManager Class
{176d6597-26d3-11d1-b350-080036a75b03}   ICM Scanner Management
{17CCA71B-ECD7-11D0-B908-00A0C9223196}   Generic WDM Filter Proxy
{17D6CCD8-3B7B-11D2-B9E0-00C04FD8DBF7}   DsObjectPicker
{17FC1A80-140E-4290-A64F-4A29A951A867}   OpenMediaSharing
{1821B62A-B2A5-4e0a-98C5-9FA0D5BAAAEC}   WMPDMCPlaylistsManager Class
{182C40F0-32E4-11D0-818B-00A0C9231C29}   COM+ Catalog Server
{1860E246-E924-4F73-B2C5-93E0577E3AA1}   IWmiCoreServices Class
{187463A0-5BB7-11D3-ACBE-0080C75E246E}   WM ASF Reader
{18907f3b-9afb-4f87-b764-f9a4e16a21b8}   CLSID_ConditionAttribute
{1890B385-5DD3-33B4-84DB-24FD1685F33D}
{18C628EE-962A-11D2-8D08-00A0C9441E20}   Xml2Dex Class
{190BA3F6-0205-4f46-B589-95C6822899D2}   MemoryDiagnosticCustomHandler
{19352205-42B0-4690-9AA4-D7DB9AE5F259}   Publication Services Change Data
{193B4137-0480-11D1-97DA-00C04FB9618A}   Microsoft DTC Transaction Unmarshaller
(private, internal)
{19603261-6059-43DF-B9E1-8B4352825A90}   scanprofileui class
{196f128d-dce9-4090-b061-3d29c6ca32c2}   Work Offline or Online
```

Page 59

SOFTWARE OUTPUT.txt

```
{19b9dcc7-6f37-4dc7-9da6-8af601c5fce2}    Mobile Broadband Media Manager
{19BA17F2-2602-4E77-9027-103894607626}    Share Media Settings Writer
{1A0391BF-9564-4294-B0A4-06C298929EF9}    Share Specific Users
{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5}    Sync Center Control
{1A34F5C1-4A5A-46DC-B644-1F4567E7A676}
{1A39680C-2376-4E8E-B168-2148D7FF9AF4}
{1A3F11DC-B514-4B17-8C5F-2154513852F1}
{1A56451B-1315-4012-861E-8587333DD631}    WMEnc Screen Capture Filter
{1A8766A0-62CE-11CF-A5D6-28DB04C10000}    WDM Streaming Standard Interface Handler
{1ab4a8c0-6a0b-11d2-ad49-00c04fa31a86}
{1AB78400-B5A3-4D91-8ACE-33FCD1499BE6}
{1AF81E4E-FC45-48ee-B236-A2A663494390}    Out Of Proc Mapi Handler
{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}    Microsoft WBEM (non)Standard Marshaling
for IEnumWbemClassObject
{1B544C20-FD0B-11CE-8C63-00AA0044B51E}    AVI Splitter
{1B544C24-FD0B-11CE-8C63-00AA0044B520}    DirectX Transform Wrapper Property Page
{1B7D4AD0-A1B1-43A8-9A46-FB36AB4C1868}    WMPDMCDevice Class
{1BA21EC2-FC80-4515-AAAB-F5766A4B88BC}    ConfigUI Class
{1BA783C1-2A30-4ad3-B928-A9A46C604C28}    Create New Link
{1BB05961-5FBF-11D2-A521-44DF07C10000}    XML Graphbuilder
{1BE1F766-5536-11D1-B726-00C04FB926AF}    EventSystemTier2
{1BE49F30-0E1B-11D3-9D8E-00C04F72D980}    BDA Tuning Model Language Component Type
Class (Broadcast Substream Type)
{1BF18D30-223C-4E0F-9074-C78C1256FD43}    Windows Media Player
WMEncAdvancedStreamEdit Class
{1C15D484-911D-11D2-B632-00C04F79498E}    Legacy Analog TV Tuner Device Segment
{1c1800c1-3258-44c2-be80-3deadb6c5e39}    CLSID_KindDescriptionFactory
{1C5221CB-C1F6-4999-8936-501C2023E4CD}    Bluetooth FD Provider
{1C621200-67B2-11D2-9EEB-006008039E37}    Black Generator Property Page
{1C82EAD9-508E-11D1-8DCF-00C04FB951F9}    Windows Mail Mime Editor
{1cedc5da-3614-11d2-bf96-00c04fd8d5b0}
{1D2680C9-0E2A-469d-B787-065558BC7D43}    Fusion Cache
{1d2b8d89-9324-46a0-b797-5725d8c8d881}    SdBackupConfig Class
{1D3529C7-671A-468d-AD2A-499A96B073D1}    AutoConfig Helper Class
{1D583ABC-8A0E-4657-9982-A380CA58FB4B}
{1d8a9b47-3a28-4ce2-8a4b-bd34e45bceeb}    UPnPDescriptionDocument Class
{1DA08500-9EDC-11CF-BC10-00AA00AC74F6}    VGA 16 color ditherer
{1DB68FCC-3C8C-49DB-8C76-9A89DE76B8CF}    WMPDMCDevicesManager Class
{1DCB3A00-33ED-11D3-8470-00C04F79DBC0}    PSFactoryBuffer
{1DF7D126-4050-47F0-A7CF-4C4CA9241333}    BDA Tuning Model DVB Satellite Locator
{1E1714A3-50B9-480b-A94A-636D9A9B56D1}    Shell Indexer Admin Object
{1E4CEC13-76BD-4ce2-8372-711CB6F10FD1}    XML Paper Specification Filter
{1E5300BE-0762-4527-8140-C0FF22DDFC56}    Parental Controls Override
{1E589E9D-8A8D-46d9-A2F9-E6D4F8161EE9}    MF MPEG Property Handler
{1E651CC0-B199-11D0-8212-00C04FC32C45}    Memory Allocator
{1E8F0D70-7399-41BF-8598-7949A2DEC898}    Microsoft DocProp Boolean Control
{1ea1ea14-48f4-4054-ad1a-e8aee10ac805}    Resizer DMO
{1ea5fb56-9ee8-47dc-8998-f45585c2e3e0}    MFPlay Class Factory
{1EC2DE53-75CC-11d2-9775-00A0C9B4D50C}    Microsoft Common Language Runtime Meta
Data
{1eeb5b5a-06fb-4732-96b3-975c0194eb39}    Itemsview
{1f01f4e9-8b75-4e20-8eb0-e49f17f2be61}    Mobile Broadband PromptPinPage Class
{1F0BC6AD-46D4-488B-BE1F-047FC7505E60}    ActualWbemAdministrativeLocator Class
{1f1f4e1a-2252-4063-84bb-eee75f8856d5}    WM Speech Encoder DMO
{1F247DC0-902E-11D0-A80C-00A0C906241A}    Content Index ISearch Creator Object
{1f26a602-2b5c-4b63-b8e8-9ea5c1a7dc2e}    SBE2MediaTypeProfile
{1f2e5c40-9550-11ce-99d2-00aa006e086c}    Security Shell Extension
{1f3427c8-5c10-4210-aa03-2ee45287d668}    User Pinned
{1f3d8aa5-9ebf-4ee4-85c2-ea40379aede8}    CScriptedDiag
{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}    Memory Mapped Cache Mgr
{1F7D1BE9-7A50-40b6-A605-C4F3696F49C0}    ThirdPartyEapDispatcherPeerConfig
{1f849cce-2546-4b9f-b03e-4004781bdc40}    CLSID_ExplorerLauncher
{1F87137D-0E7C-44d5-8C73-4EFFB68962F2}    Microsoft WMI Provider Subsystem Secured
```

Page 60

SOFTWARE OUTPUT.txt

Host
```
{1FA9085F-25A2-489B-85D4-86326EEDCD87}   Manage Wireless Networks
{1FCE6123-B675-4790-A629-F3E8AC06F839}
{20076C7E-4851-41ed-9EB8-F4E5F2BB0286}   PSFactoryBuffer
{203b1eed-db9f-40fb-87bd-1990982017d2}   WMSDK NamespaceFactory Class
{204810b9-73b2-11d4-bf42-00b0d0118b56}   UPnPRegistrar
{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29}   Microsoft OLE DB Row Position Library
{2087c2f4-2cef-4953-a8ab-66779b670495}   WinHttpRequest Component version 5.1
{208D2C60-3AEA-1069-A2D7-08002B30309D}   Network
{20b1cb23-6968-4eb9-b7d4-a66d00d07cee}   Folder View Host
{20E25881-F081-448e-85C9-4707A9400593}   User Profile WMI Provider
{21167137-B7E3-40B6-8863-8386E8C05716}   XWizard Factory Generated Class
{212690FB-83E5-4526-8FD7-74478B7939CD}   Microsoft DTV-DVD Video Decoder
{215B77BA-853F-48C4-8DC4-024E0D68A812}   SBE Stats - sender side
{216C62DF-6D7F-4E9A-8571-05F14EDB766A}   Microsoft DVBT Network Provider
{217FC9C0-3AEA-1069-A2DB-08002B30309D}   Shell Copy Hook
{21B22460-3AEA-1069-A2DC-08002B30309D}   File Property Page Extension
{21EC2020-3AEA-1069-A2DD-08002B30309D}   All Control Panel Items
{2206CDB0-19C1-11D1-89E0-00C04FD7A829}   MSDAINITIALIZE Class
{2206CDB2-19C1-11D1-89E0-00C04FD7A829}   Microsoft OLE DB Service Component Data
```
Links
```
{2206CDB3-19C1-11D1-89E0-00C04FD7A829}   MSDASC Error Lookup
{220898A1-E3F3-46B4-96EA-B0855DC968B6}   Play music command
{2227A280-3AEA-1069-A2DE-08002B30309D}   Printers
{223E7283-D39D-40d9-9BE9-AA61A39FBC5E}   Unsecured Net Connect Page Class
{228136B0-8BD3-11D0-B4EF-00A0C9138CA4}   Catalog Class
{228136B8-8BD3-11D0-B4EF-00A0C9138CA4}   Cellset Class
{22877a6d-37a1-461a-91b0-dbda5aaebc99}   Recent Places Folder
{2291478C-5EE3-4bef-AB5D-B5FF2CF58352}   MSVidCtl SBE Source to iTV Composition
```
Segment
```
{22c6c651-f6ea-46be-bc83-54e83314c67f}   Folder Infotip
{22D6F312-B0F6-11D0-94AB-0080C74C7E95}   Windows Media Player
{22D8B4F2-F577-4adb-A335-C2AE88416FAB}   PSFactoryBuffer
{22e5fca2-9c7c-4239-8aed-4d0623f532d8}   CMigrationPlugin Object
{22EE26E5-2289-11d2-8F43-00C04FC2E0C7}
{22ff30d1-a59e-4580-9190-da3042ceca64}   Mobile Broadband Roaming Page Class
{232b501c-348c-457e-972c-7c3adb1552c1}   Config Backup AutoPlay Handler Class
{233664b0-0367-11cf-abc4-02608c9e7553}   ADs Namespaces Object
{233A9694-667E-11d1-9DFB-006097D50408}   Windows Mail Address Book
{23613363-0028-431D-A49E-A3CD482D3926}   Start Menu Group PolicyFilter
{236C9559-ADCE-4736-BF72-BAB34E392196}
{23CF860E-9D2C-451A-8E83-C79C848D85A6}   PSFactoryBuffer
{242025BB-8546-48B6-B9B0-F4406C54ACFC}   InkSettings Class
{24264891-E80B-4fd3-B7CE-4FF2FAE8931F}   PSFactoryBuffer
{24400D16-5754-11d2-8218-00C04FB687DA}   Index Cleaner Prop Bag
{24D568C5-F3AE-4F91-9CD9-AA18876DA7C2}   Homegroup Control Panel
{24DC3975-09BF-4231-8655-3EE71F43837D}   Video Mixing Renderer 9 Device Segment
{25150040-b8f1-418e-af61-b51071ac1ee2}   IEnumExplorerCommand Object On Menu
{25585dc7-4da0-438d-ad04-e42c8d2d64b9}   Client application shell extension
{2559a1f0-21d7-11d4-bdaf-00c04f60b9f0}   Search
{2559a1f1-21d7-11d4-bdaf-00c04f60b9f0}   Help and Support
{2559a1f2-21d7-11d4-bdaf-00c04f60b9f0}   Windows Security
{2559a1f3-21d7-11d4-bdaf-00c04f60b9f0}   Run...
{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}   E-mail
{2559a1f7-21d7-11d4-bdaf-00c04f60b9f0}   Set Program Access and Defaults
{25ab468c-3974-4075-be50-193135461727}   Show/hide menu bar command invocation
{25BAAD81-3560-11D3-8471-00C04F79DBC0}   MediaDevMgr Class
{25BE9228-00AF-11D2-BF87-00C04FD8D5B0}
{25CBB996-92ED-457e-B28C-4774084BD562}   GenericProvider
{25E609E0-B259-11CF-BFC7-444553540000}   Microsoft DirectInput
{25E609E1-B259-11CF-BFC7-444553540000}   Microsoft DirectInputDevice
{25E609E4-B259-11CF-BFC7-444553540000}   Microsoft DirectInput8
{25E609E5-B259-11CF-BFC7-444553540000}   Microsoft DirectInput8
```
Page 61

```
                    SOFTWARE  OUTPUT.txt
  {26671179-2ec2-42bf-93d3-64108589cad5}  ShellItemArray Shell Namespace helper
  {266EEE40-6C63-11cf-8A03-00AA006ECB65}  WDM TV Tuner
  {266EEE41-6C63-11cf-8A03-00AA006ECB65}  TV Tuner Property Page
  {267cf8a9-f4e3-41e6-95b1-af881be130ff}  Location Folder
  {267DB0B3-55E3-4902-949B-DF8F5CEC0191}  Custom Composition Segment from WebDVD
Device Segment to Standard Video Renderer Device Segment
  {26EC0B63-AA90-458A-8DF4-5659F2C8A18A}  BDA Tuning Model Digital Cable Tune
Request
  {26EE0668-A00A-44D7-9371-BEB064C98683}  Control Panel
  {26fdc864-be88-46e7-9235-032d8ea5162e}  Merged Folder
  {271C3902-6095-4c45-A22F-20091816EE9E}  MPEG4 Byte Stream Handler
  {273eb5e7-88b0-4843-bfef-e2c81d43aae5}  Application Startup Link
  {275C23E2-3747-11D0-9FEA-00AA003F8646}  Multi Language Support
  {2764BCE5-CC39-11D2-B639-00C04F79498E}  Generic Graph Composition Segment
  {2769280B-5108-498c-9C7F-A51239B63147}  PSFactoryBuffer
  {276FBFC1-D71F-4619-A7C1-0181077EE283}  Microsoft.Windows.Diagnosis.ManagedHost
  {2781761E-28E0-4109-99FE-B9D127C57AFE}  Windows Defender IOfficeAntiVirus
implementation
  {27949969-876A-41D7-9447-568F6A35A4DC}
  {280A3020-86CF-11D1-ABE6-00A0C905F375}  AC3 Parser Filter
  {288a2d5f-253c-46b4-b58c-2ced3180b993}  CMI IInstaller
  {289228DE-A31E-11D1-A19C-0000F875B132}  ListPad class
  {28953661-0231-41DB-8986-21FF4388EE9B}  MSVidCtl Analog Capture to Encoder
Composition Segment
  {289978AC-A101-4341-A817-21EBA7FD046D}  Sync Center Conflict Folder
  {28AB0005-E845-4FFA-AA9B-F4665236141C}  Analog Audio Component Type
  {28AF2E16-0190-44F4-9CED-08AF91145361}  RA Helper Class
  {291EE2A7-BFA5-4e9e-A358-C93655556A6C}  VideoProcAmp2 Class
  {2933BF90-7B36-11D2-B20E-00C04F983E60}  XML DOM Document
  {2933BF91-7B36-11D2-B20E-00C04F983E60}  Free Threaded XML DOM Document
  {2933BF94-7B36-11D2-B20E-00C04F983E60}  XSL Template
  {2965e715-eb66-4719-b53f-1672673bbefa}  Results Folder
  {2981c306-09ea-405d-9d0f-83337827bd35}
  {29B5828C-CAB9-11D2-B35C-00105A1F8177}  Microsoft WBEM (non)Standard Marshaling
for IWbemUnboundObjectSink
  {29F06F0C-FB7F-44A5-83CD-D41705D5C525}  NCProvider Class
  {2A005C11-A5DE-11CF-9E66-00AA00A3F464}  PropGroupManagerObject Class
  {2a11bae2-fe6e-4249-864b-9e9ed6e8dbc2}  Mpeg4s Decoder DMO
  {2A11F42C-3E81-4ad4-9CBE-45579D89671A}  CivicAddressReportFactory Class
  {2A196062-812A-4249-B04A-797971DC466C}  XML Paper Specification Filter Persistent
Handler
  {2A2699C5-775A-42e9-BF4A-A36FE41BA4CB}  TCPIProp Class
  {2A614240-A4C5-4C33-BD87-1BC709331639}  Bidi Spooler APIs
  {2A6F3A80-5976-11D2-9524-0060081840BC}  Silence
  {2A744BD8-158A-4bbf-9513-4A656F6C01D7}  Windows Desktop Search Scope Manager
  {2af6bcaa-f526-4803-aeb8-5777ce386647}  EapMschapv2Cfg Class
  {2B20FE1A-1B2C-4DC5-8595-616B0E182FD1}  MSASR Locale Handler Class (1036)
  {2B362208-CB07-4fa5-8076-8DB4AA890561}  WMPDMCServer Class
  {2B4B0612-E1F4-376F-A9B9-86BA3F72A670}
  {2BD40F38-DE45-429D-9D04-24F7C24C78FD}  PSFactoryBuffer
  {2C256447-3F0D-4CBB-9D12-575BB20CDA0A}  FaultrepElevatedDataCollection
  {2C2CEA16-CC79-4C01-B3CE-B5B7CE47101F}  Microsoft IME IMEPad interface
  {2C63E4EB-4CEA-41B8-919C-E947EA19A77C}  BDA Tuning Model MPEG2 Tune Request
Factory
  {2C673043-FC2E-4d67-8920-517D24DEBD2C}
  {2C676B7B-796E-4C59-8209-4D0473E32A17}  WMEncSourceSink
  {2C731933-62A6-31A0-AFE1-1034F46361D2}
  {2C875213-FCE5-11d1-A0B0-00C04FA31A86}
  {2CA8CA52-3C3F-11D2-B73D-00C04FB6BD3D}  AudioInputMixer Property Page
  {2D11CF10-4FE0-45B2-88DF-6FFBF92BE9AB}  WaitDialog
  {2D1F634B-BA35-4BA0-A3B4-B03AC5FE724A}  DUN Device Center Context Menu Handler
  {2D2E24CB-0CD5-458F-86EA-3E6FA22C8E64}  VMR Allocator Presenter 9
  {2d3468c1-36a7-43b6-ac24-d3f02fd9607a}  A collection of IUnknown objects that can
                         Page 62
```

SOFTWARE OUTPUT.txt

be enumerated

```
{2DB47AE5-CF39-43C2-B4D6-0CD8D90946F4}    StreamBufferSink
{2DB5E62B-0D67-495F-8F9D-C2F0188647AC}
{2DD80115-AD1E-41F6-A219-A4F4B583D1F9}    PSFactoryBuffer
{2DEA658F-54C1-4227-AF9B-260AB5FC3543}    Microsoft PlaySoundService Class
{2E095DD0-AF56-47e4-A099-EAC038DECC24}    AnalogCable Class
{2e167ea7-85e3-4395-995a-77af9875d79a}
{2E17C0EF-2851-459b-A3C8-27A41D4BC9F7}    Windows Theme Manager API
{2e5e84e9-4049-4244-b728-2d24227157c7}    UPnPRemoteEndpointInfo
{2e7583c7-7eba-4a1a-8468-d03d28477e6f}    Shell settings migration
{2E9E59C0-B437-4981-A647-9C34B9B90891}    Sync Setup Folder
{2EBDEE67-3505-43f8-9946-EA44ABC8E5B0}    PSFactoryBuffer
{2ED326ED-C4C0-434a-B4CE-FB0318D725A7}    PSFactoryBuffer
{2eeb4adf-4578-4d10-bca7-bb955f56320a}    WMAudio Decoder DMO
{2EEEED04-0908-4cdb-AF8F-AC5B768A34C9}    Drm Scheme Handler
{2F2165FF-2C2D-4612-87B2-CC8E5002EF4C}    Advanced Indexing Options Dialog Object
{2f2dc38b-34d2-462c-add4-f74cc15510a1}    SuggestPopup
{2F94D7B0-BF63-11D1-A6A2-00C04FB9988E}    EndpointsTable Class
{2FB21955-33A2-46A0-8F60-B475DC33FD5A}    PSFactoryBuffer
{2FE9B39E-0062-41E5-A842-518E212C2CE0}    PSFactoryBuffer
{301056D0-6DFF-11D2-9EEB-006008039E37}    MJPEG Decompressor
{3037B4CD-A40B-401B-B676-2017EE8FAFF4}    Wordpad DOCX Filter
{30766BD2-EA1C-4F28-BF27-0B44E2F68DB7}    Windows Search Root
{3080F90D-D7AD-11D9-BD98-0000947B0257}    Show Desktop
{3080F90E-D7AD-11D9-BD98-0000947B0257}    Window Switcher
{30d49246-d217-465f-b00b-ac9ddd652eb7}    Identity Store
{3124C396-FB13-4836-A6AD-1317F1713688}    SAX XML Reader 3.0
{3140F5B6-093F-4F94-9141-5DF9EE10BC27}    MSASR Locale Handler Class (1033)
{31430c59-bed1-11D1-8De8-00C04FC2E0C7}
{317E92FC-1679-46FD-A0B5-F08914DD8623}    InstallationAgent Class
{317F3AA1-A5F5-4310-9401-BAE5DAC386C6}    text persistent handler for mapi email
{31879719-E751-4DF8-981D-68DFF67704ED}
{31b11d80-9ed7-44f7-b1cd-c95992a738b9}    Layer Composer
{31b231f6-546d-4f9b-ac95-0f963d72559c}    Sync Command State Handler
{31DCBC0C-20D8-40b0-A409-F4474A942358}    TcpiObj Class
{323CA680-C24D-4099-B94D-446DD2D7249E}    Favorites
{32557D3B-69DC-4F95-836E-F5972B2F6159}
{32624F4B-F1D5-4877-989E-555640109D2B}    Windows Photo Viewer Gallery Interface
{32714800-2E5F-11d0-8B85-00AA0044F941}    For &People...
{3283EEBF-E67D-31AC-8481-A968F3A77E9A}
{328B0346-7EAF-4BBE-A479-7CB88A095F5B}    LayoutFolder
{32BAED44-34B5-11D3-9315-00C04F72D6CF}    MSSCP Class
{32C5A81F-27C0-4E66-A894-786F646F1236}    PSFactoryBuffer
{32d186a7-218f-4c75-8876-dd77273a8999}    Microsoft AAC Audio Decoder MFT
{32DA2B15-CFED-11D1-B747-00C04FC2B085}    Script Encoder Object
{32E7DC13-1E22-4D7E-8AC7-D2E718DE8042}    InfraProfileExistsErrorPage
{3336B8BF-45AF-429f-85CB-8C435FBF21E4}    ClassicW Class
{334125C0-77E5-11D3-B653-00C04F79498E}    BDA Data Services Feature Segment
{334857cc-f934-11d2-ba96-00c04fb6d0d1}    ADs DN With String Object
{336475D0-942A-11CE-A870-00AA002FEAB5}    MPEG-I Stream Splitter
{33BCC8EC-0D01-4E10-AD3D-4DAF749873ED}    Browser Application State
{33C4643C-7811-46FA-A89A-768597BD7223}    PSFactoryBuffer
{33C53A50-F456-4884-B049-85FD643ECFED}    TF_InputProcessorProfiles
{33c86cd6-705f-4ba1-9adb-67070b837775}    Onex PLAP Smartcard Credential Provider
{33D9A760-90C8-11D0-BD43-00A0C911CE86}
{33D9A761-90C8-11d0-BD43-00A0C911CE86}    ACM Class Manager
{33D9A762-90C8-11d0-BD43-00A0C911CE86}    WaveIn Class Manager
{33de48c4-943f-4b96-8cd8-b117c94576cf}
{33FACFE0-A9BE-11D0-A520-00A0D10129C0}    SAMI (CC) Reader
{343D770D-7788-47c2-B62A-B7C4CED925CB}    WpcNotificationsMigration
{348C9CFF-CB90-4024-AE22-F17259A3934B}    WlanBalloonHandler Class
{34A19196-274E-4D75-9D30-D7A45A0A4178}    Windows Live Services Class
{34c219bd-85c1-4338-95e8-788a36901dc2}    Configure Windows Portable Device Task
```

Page 63

SOFTWARE OUTPUT.txt

```
Class
    {3508C064-B94E-420b-A821-20C8096FAADC}   AtscPsipParser Class
    {35117bca-71f9-4399-8709-f380c7aaa8bd}   Screen Fade
    {35298344-96A6-45E7-9B6B-62ECC6E09920}   PSFactoryBuffer
    {3529B1D2-313A-4202-BD3E-5996B7E18A10}
    {352EC2B7-8B9A-11D1-B8AE-006008059382}   Shell Application Manager
    {3540D440-5B1D-49cb-821A-E84B8CF065A7}   MSVidCtl Analog Capture to XDS Composition
Segment
    {354F7156-A4F6-47F5-A028-FE2000E92132}   PSFactoryBuffer
    {355DFFAA-3B9F-435c-B428-5D44290BC5F2}   WpcSettingsProvider Class
    {356F2F88-05A6-4728-B9A4-1BFBCE04D838}
    {35786D3C-B075-49b9-88DD-029876E11C01}   Portable Devices
    {35C61CC2-5851-4F2D-89B6-4F9BB4B4193F}   Microsoft Search Property System Change
Notify Handler
    {3692CA39-E082-4350-9E1F-3704CB083CD5}
    {3697790B-223B-484E-9925-C4869218F17A}
    {36eef7db-88ad-4e81-ad49-0e313f0c35f8}   Windows Update
    {36f0bd14-d84d-468c-b79c-9990f3fa897f}   Multi Object Elevation Factory
    {370A1D5D-DDEB-418C-81CD-189E0D4FA443}   VBI Codec
    {372FCE38-4324-11D0-8810-00A0C903B83C}   CertConfig Class
    {3730bbf8-631a-48fb-9085-e2143c11563b}   XWizard Factory Generated Class (HomeGroup
Empty Hook Page)
    {3734FF83-6764-44B7-A1B9-55F56183CDB0}   Sync Center (Internal)
    {373984C9-B845-449B-91E7-45AC83036ADE}   XML Schema Cache
    {3756e7f5-e514-4776-a32b-eb24bc1efe7a}   State of built-in commands
    {375ff002-dd27-11d9-8f9c-0002b3988e81}   WCN-Config Function Discovery Provider
Class
    {37734C4D-FFA8-4139-9AAC-60FBE55BF3DF}   BlbEngine Class
    {379E501F-B231-11D1-ADC1-00805FC752D8}   MsxmlIsland
    {37A61C8B-7F8E-4d08-B12B-248D73E9AB4F}   Secure Http Scheme Handler
    {37B0353C-A4C8-11D2-B634-00C04F79498E}   File Playback Device Segment
    {37B03543-A4C8-11D2-B634-00C04F79498E}   Standard Video Renderer Device Segment
    {37B03544-A4C8-11D2-B634-00C04F79498E}   Standard Audio Renderer Device Segment
    {37de7045-5056-456f-8409-c871e0f8b0e0}   Trun Gateway Protocol Class
    {37E92A92-D9AA-11D2-BF84-8EF2B1555AED}   Audio Renderer Advanced Properties
    {37ea3a21-7493-4208-a011-7f9ea79ce9f5}   Open Containing Folder Menu
    {37efd44d-ef8d-41b1-940d-96973a50e9e0}   Windows Sidebar Properties
    {380BA9E8-E1E6-33C3-8CA9-385FA6E48C88}
    {381DDA3C-9CE9-4834-A23E-1F98F8FC52BE}
    {384ea5ae-ade1-4e8a-8a9b-7bea78fff1e9}   CLSID_BinaryAutoList
    {3882134d-14cf-4220-9cb4-435f86d83f60}   PortableDeviceValuesCollection Class
    {389EA17B-5078-4CDE-B6EF-25C15175C751}
    {38A98528-6CBF-4CA9-8DC0-B1E1D10F7B1B}
    {38F03426-E83B-4E68-B65B-DCAE73304838}   Custom Composition Segment from Data
Services to Time Shift Sink
    {3901CC3F-84B5-4FA4-BA35-AA8172B8A09B}   DirectSound 8.0 Object
    {3908C3CD-4478-4536-AF2F-10C25D4EF89A}   WiaVideo Class
    {39981129-C287-11D0-8D8C-00C04FD6202B}   CLSID_CMAPIAcctImport
    {39AE2AEA-D4D5-4DA0-AE47-C020E1BE4BE5}   CLSID_JetDatabaseSession
    {39F8D76B-0928-11D1-97DF-00C04FB9618A}   Microsoft DTC Transaction
    {3A614B00-FB18-46F3-950E-682A46A48B9F}   PSFactoryBuffer
    {3A8CCCBC-0EFD-43a3-B838-F38A552BA237}   CTocEntryList
    {3A9428A7-31A4-45E9-9EFB-E055BF7BB3DB}   BDA Tuning Model Channel ID Tune Request
    {3ABEAFC4-F48F-4517-A9B0-8AD6A94A99A1}   Publication Services Data
    {3ad05575-8857-4850-9277-11b85bdb8e09}   Copy/Move/Rename/Delete/Link Object
    {3ADCE5CC-13C8-4573-B328-ED438EB694F9}   CAviTocParser
    {3AE86B20-7BE8-11D1-ABE6-00A0C905F375}   MPEG-2 Splitter
    {3B881B82-5BF4-4657-A3A2-CCE17E4FD39A}   Nap Server Info class
    {3bb4118f-ddfd-4d30-a348-9fb5d6bf1afe}   Time Categorizer
    {3BBE95A4-C53F-11d1-B3A2-00A0C9083365}   TRUN Tx Begin Class
    {3BBE95DA-C53F-11d1-B3A2-00A0C9083365}   Trun Gateway Tx Class
    {3BBE95F5-C53F-11d1-B3A2-00A0C9083365}   Trun Gateway Tx Crash Recovery Class
    {3BBE95FB-C53F-11d1-B3A2-00A0C9083365}   Trun Gateway Instance Class
```

Page 64

SOFTWARE OUTPUT.txt

```
{3BBE95FE-C53F-11d1-B3A2-00A0C9083365}    Trun Gateway Instance Scan Class
{3c2654c6-7372-4f6b-b310-55d6128f49d2}    Alphabetical Categorizer
{3C305196-50DB-11D3-9CFE-00C04FD930C5}    DirectDraw7 Object
{3C3A70A7-A468-49B9-8ADA-28E11FCCAD5D}    RASrv Class
{3C4708DC-B181-46A8-8DA8-4AB0371758CD}    MSVidCtl SBE Source to Video Mixing
Renderer Composition Segment
{3C5F432A-EF40-4669-9974-9671D4FC2E12}    MMC Plugable Internet Protocol
{3CCF8A41-5C85-11d0-9796-00AA00B90ADF}    Shell DeskBarApp
{3CE74DE4-53D3-4D74-8B83-431B3828BA53}    TF_DisplayAttributeMgr
{3D07A539-35CA-447C-9B05-8D85CE924F9E}    Closed Captions Analysis Filter
{3D112E22-62B2-11D1-9FEF-00600832DB4A}    MMCTask class
{3d154a2d-d911-437e-a30c-5f56a9b7081d}    Extract Const Icon Handler
{3D813DFE-6C91-4A4E-8F41-04346A841D9C}    MXXMLWriter 3.0
{3D96ED94-5D75-4165-9E1F-1A642C7BA316}    Windows Media Player WMEncTextInputSource
Class
{3dad6c5d-2167-4cae-9914-f99e41c12cfa}    Include In Library Sub Context Menu
{3dd6bec0-8193-4ffe-ae25-e08e39ea4063}    NPProvider
{3DD82D10-E6F1-11D2-B139-00105A1F77A1}    WMI instrumentation:
Win32_PowerManagementEvent
{3E000D72-A845-4CD9-BD83-80C07C3B881F}    CMLUAUTIL
{3E458037-0CA6-41aa-A594-2AA6C02D709B}    SBE2FileScan
{3E4D4F1C-2AEE-11D1-9D3D-00C04FC30DF6}    oleprn Class
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}    CMSTPLUA
{3E784A01-F3AE-4DC0-9354-9526B9370EBA}    SAXAttributes 3.0
{3EE60F5C-9BAD-4CD8-8E21-AD2D001D06EB}    InkObject Class
{3eef301f-b596-4c0b-bd92-013beafce793}    Destkop Undo Manager
{3EF76D68-8661-4843-8B8F-C37163D8C9CE}    Custom Composition Segment from CCA to
Stream Buffer Source
{3F281000-E95A-11d2-886B-00C04F869F04}    Com Call Wrapper Unmarshal Class
{3F35F070-99D6-11D2-8D10-00A0C9441E20}    Audio Repackager
{3f454f0e-42ae-4d7c-8ea3-328250d6e272}    Automation context menu
{3F6953F0-5359-47FC-BD99-9F2CB95A62FD}    Personal Start Menu
{3f6bc534-dfa1-4ab4-ae54-ef25a74e0107}    System Restore
{3FC0B520-68A9-11D0-8D77-00C04FD70822}    Display Control Panel HTML Extensions
{3FF292B6-B204-11CF-8D23-00AA005FFE58}    FoxOLEDB 1.0 Object
{3FF566F0-6E6B-49D4-96E6-B78886692C62}
{3FFB3B8C-EB99-472b-8902-E1C1B05F07CF}    LPCM Byte Stream Handler
{4003191F-71FF-49A2-B591-05C606FADB8B}    WMPlayer MusicPropPage Class
{40419485-C444-4567-851A-2DD7BFA1684D}    Phone and Modem Control Panel
{404A6DE5-D4D6-4260-9BC7-5A6CBD882432}
{40C3D757-D6E4-4b49-BB41-0E5BBEA28817}    Video Media Properties Handler
{40dd6e20-7c17-11ce-a804-00aa003ca9f6}    Shell extensions for sharing
{41070793-59E4-479A-A1F7-954ADC2EF5FC}
{4125dd96-e03a-4103-8f70-e0597d803b9c}    Microsoft Attachment Services
{41457294-644C-4298-A28A-BD69F2C0CF3B}    ASF Byte Stream Handler
{417BAB8B-9D22-4A88-9DA0-98C4AB6745D5}    WPD Settings Commit Page Class
{418008F3-CF67-4668-9628-10DC52BE1D08}    BDA Tuning Model MPEG2 Component Type
Class (Broadcast Substream Type)
{418AFB70-F8B8-11CE-AAC6-0020AF0B99A3}    Quality Management Property Page
{418c8b64-5463-461d-88e0-75e2afa3c6fa}    Explorer Browser Results Folder
{41937347-2aba-4d4c-a4ca-6fe4f11f1bac}    Network Item Factory
{41B23C28-488E-4E5C-ACE2-BB0BBABE99E8}    HHCtrl Object
{41B9BE05-B3AF-460C-BF0B-2CDD44A093B1}    XML filter
{41E300E0-78B6-11ce-849B-444553540000}    Display Effects CPL Extension
{42044394-8c34-11d1-83bc-00c04fbbc34e}
{42150CD9-CA9A-4EA5-9939-30EE037F6E74}    Microsoft MPEG-2 Video Encoder
{424bed78-ef88-4b7c-945c-b8cf46d56e20}    Authentication UI Last Logged On Username
{427BC7E3-F833-4584-8745-CFAB9D7A5761}    CTaskConditionCombiner
{427FD3D4-F30A-4033-84EF-CBB1A955D9F7}    AggregateAssociationList
{42aedc87-2188-41fd-b9a3-0c966feabec1}    MruPidlList
{42C9B9F5-16FC-47ef-AF22-DA05F7C842E3}    WAV Byte Stream Handler
{42DFB618-A403-4401-908F-FE979B2215C8}    PSFactoryBuffer
{43136EB5-D36C-11CF-ADBC-00AA00A80033}    NodeInit 1.0 Object
```

Page 65

SOFTWARE OUTPUT.txt

```
{4315D437-5B8C-11D0-BD3B-00A0C911CE86}   DeviceMoniker
{43232233-8338-4658-ae01-0b4ae830b6b0}   PortableDeviceDispatchFactory Class
{43324B33-A78F-480F-9111-9638AACCC832}
{4336a54d-038b-4685-ab02-99bb52d3fb8b}   Public Folder
{435899C9-44AB-11D1-AF00-080036234103}   DSPrintQueue Class
{437ff9c0-a07f-4fa0-af80-84b6c6440a16}   Command Folder
{43B07326-AAE0-4B62-A83D-5FD768B7353C}   InkRectangle Class
{43FB1553-AD74-4ee8-88E4-3E6DAAC915DB}   InkCollector Class
{4405b37b-60fe-49ed-ba8f-691a78f84daf}
{44121072-A222-48f2-A58A-6D9AD51EBBE9}
{443E7B79-DE31-11D2-B340-00104BCC4B4A}   WbemUnauthenticatedLocator Class
{4444AC9E-242E-471B-A3C7-45DCD46352BC}   VMR Allocator Presenter DDXcl Mode
{44CB442B-9DA9-49df-B3FD-023777B16E50}   Http Scheme Handler
{44da8435-b187-4dd6-8f32-9341eb7e4c3c}   CLSID_CSmapiProxy
{44EC053A-400F-11D0-9DCD-00A0C90391D3}   Registrar Class
{44f3dab6-4392-4186-bb7b-6282ccb7a9f6}   MyDocuments menu and properties
{44F9A03B-A3EC-4F3B-9364-08E0007F21DF}   TaskSymbol Class
{4522c772-9a2b-4920-ad7f-62d3d15eac52}   Restore Default Favorite Links Command
{45597c98-80f6-4549-84ff-752cf55e2d29}   Add to Windows Media Player list
{455ACF57-5345-11D2-99CF-00C04F797BC9}   PSFactoryBuffer
{455f6102-c83a-4d07-ba36-b6da9d589ae2}   RdpAudioSink Class
{45670FA8-ED97-4F44-BC93-305082590BFB}   Microsoft XPS Shell Metadata Handler
{4582746F-473B-4022-A7E9-887CBEDD8F85}   SBE IO counters
{4582eba9-6aa1-4d79-824e-728929ef455d}   Xwizard Factory Generated Class
{4590F811-1D3A-11D0-891F-00AA004B2E24}   WBEM Locator
{4590F812-1D3A-11D0-891F-00AA004B2E24}   Microsoft WBEM WbemClassObject Marshalling
proxy
{461CDD3F-D54E-4033-A0AA-6CD24F152AA1}   WlanDlg Get Key UI Page Class
{4657278A-411B-11d2-839A-00C04FD918D0}   Shell Drag and Drop helper
{4662DAB0-D393-11D0-9A56-00C04FB68B66}
{46763EE0-CAB2-11CE-8C20-00AA0051E5D4}   Obsolete Font
{469afbdf-084f-4dc9-904f-9e824c48bc37}   Folder Initialization Handler
{46C0A7DC-928A-485a-959F-1F9EF8686A11}
{46C166AA-3108-11D4-9348-00C04F8EEB71}   Home Networking Configuration Manager
{47135eea-06b6-4452-8787-4a187c64a47e}   SdrRestoreService Class
{47354492-827E-4b8a-B318-C80EBA1381F0}   CClusterDetectorEx
{4753da60-5b71-11cf-b035-00aa006e0975}   ADs Provider Object
{477EC299-1421-4bdd-971F-7CCB933F21AD}   File Scheme Handler
{47D4D946-62E8-11cf-93BC-444553540000}   DirectSound Object
{48025243-2D39-11CE-875D-00608CB78066}   Internal Text Renderer
{480FF4B0-28B2-11D1-BEF7-00C04FBF8FEF}   DirectMusicCollection
{48123bc4-99d9-11d1-a6b3-00c04fd91555}   XML Document
{48527bb3-e8de-450b-8910-8c4099cb8624}   Empty Recycle Bin verb invocation
{489331DC-F5E0-4528-9FDA-45331BF4A571}   CInitiateWinSAT Class
{48e2ed0f-98c2-4a37-bed5-166312ddd83f}   MFReadWrite Class Factory
{48e7caab-b918-4e58-a94d-505519c795dc}   Start Menu Folder
{49010C18-B110-421a-9047-ADCA421CBC40}   IMRequestRA Class
{49638B91-48AB-48B7-A47A-7D0E75A08EDE}   BDA Tuning Model Analog Locator
{498B0949-BBE9-4072-98BE-6CCAEB79DC6F}   SmartRenderEngine Class
{4991d34b-80a1-4291-83b6-3328366b9097}   Background Intelligent Transfer Control
Class 1.0
{499EAEEA-2737-4849-8BB6-47F107EAF358}   CTocParser
{49ACAA99-F009-4524-9D2A-D751C9A38F60}   PSFactoryBuffer
{49B2791A-B1AE-4C90-9B8E-E860BA07F889}   MMC Application Class
{49BD2028-1523-11D1-AD79-00C04FD8FDFF}   Microsoft WBEM Unsecured Apartment
{49C407EF-78B9-4C82-A40B-2FE02F8E771D}   Windows Theme Thumbnail Preview
{49eb6558-c09c-46dc-8668-1f848c290d0b}   Scope Picking Dialog
{49f171dd-b51a-40d3-9a6c-52d674cc729d}   UIAutomationCrossBitnessHook64 Class
{49F371E1-8C5C-4d9c-9A3B-54A6827F513C}   Sharing Configuration Manager
{4a04656d-52aa-49de-8a09-cb178760e748}   Recycle Bin Manager
{4A16043F-676D-11d2-994E-00C04FA309D4}   CLSID_DatabaseSession
{4A1E5ACD-A108-4100-9E26-D2FAFA1BA486}   IGD Property Page
{4A2286E0-7BEF-11CE-9BD9-0000E202599C}   MPEG Audio Codec
```

Page 66

SOFTWARE OUTPUT.txt

```
{4A38E4EF-F55B-4A59-8F02-BDEFB0B1308A}   CGNPMpeg2DataControl
{4A56AF32-C21F-11DB-96FA-005056C00008}
{4A5869CF-929D-4040-AE03-FCAFC5B9CD42}   Generic Sink Segment
{4A65D267-1539-4BD1-921D-1C49B3E58EB7}   SnapInFailureReporter
{4A6B8BAD-9872-4525-A812-71A52367DC17}   RasGcw LUA
{4a714c8e-e664-4024-9c74-1a82a3da842a}   Authentication UI Background
{4a76b469-7b66-4dd4-ba2d-ddf244c766dc}   GSM ACM Wrapper MFT
{4a7ded0a-ad25-11d0-98a8-0800361b1103}   MyFolder menu and properties
{4AF3F4A4-06C8-4B79-A523-633CC65CE297}   WBEM Disk Quota Volume Provider
{4AF4A5FC-912A-11D1-B945-00A0C90312E1}   Microsoft Docking Bar Property Bag
{4B181F0F-48C8-4e80-A2AF-E3099AAC069B}   PresentationHost in-proc handler
{4B2E958D-0393-11D1-B1AB-00AA00BA3258}   COM+ Active Process Iteration Server
{4B534112-3AF6-4697-A77C-D62CE9B9E7CF}   Sync Center Event Properties Extension
{4B59AFCC-B8C3-408A-B670-89E5FAB6FDA7}
{4b6657e4-b973-46cd-9bb3-6e5ebd82448f}   PortableDeviceWMDRM Class
{4B966436-6781-4906-8035-9AF94B32C3F7}   SPP Class
{4BDD6232-2E55-4A1F-AAAD-961D76F439BA}   PSFactoryBuffer
{4bec2015-bfa1-42fa-9c0c-59431bbe880e}   Shell URL
{4C4A5E40-732C-11D0-8816-00A0C903B83C}   CertServerPolicy Class
{4C596AEC-8544-4082-BA9F-EB0A7D8E65C6}   CivicAddress Report Class
{4c649c49-c48f-4222-9a0d-cbbf4231221d}   Photo Printing with Templates Wizard
{4c892621-6757-4fe0-ad8c-a6301be7fba2}   Windows Settings Page
{4cadfae1-5512-456a-9d65-5b5e7e9ca9a3}   PortableDeviceClassExtension Class
{4CB43D7F-7EEE-4906-8698-60DA1C38F2FE}   UpdateSession Class
{4CFC7932-0F9D-4BEF-9C32-8EA2A6B56FCB}   Microsoft WMI Provider Subsystem Decoupled
Registrar
{4D111E08-CBF7-4f12-A926-2C7920AF52FC}   Shell Security Editor
{4D317113-C6EC-406A-9C61-20E891BC37F7}   RASettingProperty Class
{4D73E9D0-4716-3585-BE8B-7FF800EE5866}
{4DB1AD10-3391-11D2-9A33-00C04FA36145}   PSFactoryBuffer
{4DD1D1C3-B36A-4eb4-AAEF-815891A58A30}   Vector Class
{4DD441AD-526D-4A77-9F1B-9841ED802FB0}   SAXAttributes
{4DDA1941-77A0-4fb1-A518-E2185041D70C}   CTocGeneratorDmo
{4DE225BF-CF59-4CFC-85F7-68B90F185355}   Microsoft WMI Provider Subsystem
{4df0c730-df9d-4ae3-9153-aa6b82e9795a}   Known Folder Manager
{4DF929E7-4C5E-4587-A598-7ED7B3D6E462}   AddMdmObj Class
{4E14FBA2-2E22-11D1-9964-00C04FBBB345}   Event System
{4E40F770-369C-11d0-8922-00A024AB2DBB}   Security Shell Extension
{4ea9a1b7-e521-4813-a9f8-ba6484902cb5}   SMB Helper Class
{4EFE2452-168A-11d1-BC76-00C04FB9453B}   MidiOut Class Manager
{4F4DB904-CA35-4A3A-90AF-C9D8BE7532AC}   RecoExt Class
{4F58F63F-244B-4c07-B29F-210BE59BE9B4}   .group shell extension handler
{4F664F91-FF01-11D0-8AED-00C04FD7B597}   OleSNMP Class
{4F695794-BFCF-48B0-A323-F874F9BD45F2}   Windows Media Player
WMEncFileTransferSource Class
{4FA18276-912A-11D1-AD9B-00C04FD8FDFF}   InProcWbemLevel1Login Class
{4FAF64F1-A3BA-4172-B922-E6A22ACF7E3D}   XWizard Factory Generated Class
{4FD2A832-86C8-11D0-8FCA-00C04FD9189D}
{4FDEF69C-DBC9-454e-9910-B34F3C64B510}   PSFactoryBuffer
{4FE24495-28CE-4920-A4C4-E556E1F0DF2A}   CToc
{4FF2FE0E-E74A-4B71-98C4-AB7DC16707BA}
{50040C1D-BDBF-4924-B873-F14D6C5BFD66}   MediaDevMgrClassFactory Class
{5058292D-A244-4840-AB44-480975C4FFE4}   CTocCollection
{5068B32E-DFE0-48C2-9816-4549033447DB}   PSFactoryBuffer
{506D89AE-909A-44f7-9444-ABD575896E35}   DxtAlphaSetter Class
{5088B39A-29B4-4d9d-8245-4EE289222F66}   QueryParserManager Class
{50B1904B-F28F-4574-93F4-0BADE82C69E9}
{50cc2c18-b48c-4764-8f3f-0331ed295ce4}   Undo command invocation
{50D42F09-ECD1-4B41-B65D-DA1FDAA75663}
{510C4E33-05D5-438B-9852-E8406EFF033D}   PSFactoryBuffer
{51372af3-cae7-11cf-be81-00aa00a2fa25}   MTSPackage
{51653423-E62D-4FF7-894A-DABB2B8E21E2}   CrawlStartPages Task Handler
{517F6AA6-D6FA-46D0-8094-17FF17E4CCF4}   HomeGroup Security Hosted Listener
```

Page 67

```
                      SOFTWARE OUTPUT..txt
{51B4ABF3-748F-4E3B-A276-C828330E926A}  Video Mixing Renderer 9
{5210f8e4-b0bb-47c3-a8d9-7b2282cc79ed}  WMAPro over S/PDIF DMO
{522e34a4-07f7-40a1-94d0-1bfe832efc3a}  PSFactoryBuffer
{524B13ED-2E57-40B8-B801-5FA35122EB5C}  DrawAttrs Class
{5255EFED-103A-4444-B124-F88F99E4EF8D}  HomeGroup Printer Hosted Listener
{527c9a9b-b9a2-44b0-84f9-f0dc11c2bcfb}  Microsoft DocProp Static Property Control
{52968B13-8F33-33DB-B55F-ED57D7D05E8A}
{529A9E6B-6587-4F23-AB9E-9C7D683E3C50}  TF_ThreadMgr
{52A2AAAE-085D-4187-97EA-8C30DB990436}  HHCtrl Object
{52ce2fe5-04c3-42fd-8a8b-4251affb8408}  CLSID_ResultSetManager
{52CFFDFE-A115-4164-AFB1-EAD719C52C15}  Biometrics Policy object
{52e4e90a-f4af-460a-9e60-fdfb86c9dd5d}  Windows Media Player WMEncoder Class
{52F15C89-5A17-48e1-BBCD-46A3F89C7CC2}  LeafCondition Class
{52FD5C49-A63D-45EC-8687-98DA8B7BFE6A}  video clips pix command support
{5323BCB5-0431-42be-A482-5EE76F243A28}
{5326dddc-ec38-428d-b219-ce6dadb35de3}  Connect to a network
{53362C64-A296-4F2D-A2F8-FD984D08340B}  RemoteProxyFactory32 Class
{53445BED-3213-453B-A12A-79AA20A702DC}  LegacyPrintUI Class
{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}  Control Panel command object for Start
menu and desktop
{53a01e9d-61cc-4cb0-83b1-31bc8df63156}  Microsoft DocProp Icon List Control
{53bd6b4e-3780-4693-afc3-7161c2f3ee9c}  MruLongList
{53BEDF0B-4E5B-4183-8DC9-B844344FA104}  MAPI Mail Previewer
{53C74826-AB99-4d33-ACA4-3117F51D3788}
{5408B2F0-C816-11D1-8F99-00600895E7D5}  Interface Proxy Stub
{545AE700-50BF-11D1-9FE9-00600832DB4A}  MMCCtrl class
{548968f5-17f7-4751-a581-ff0f1c732995}  Authentication UI System Settings
{5491AB67-AFEB-48B1-B8DF-B2D63810EF40}  PSFactoryBuffer
{549365d0-ec26-11cf-8310-00aa00b505db}  ADsDSOObject
{54A05253-96FA-4B98-B8FD-9534D7255914}  PSFactoryBuffer
{54D8502C-527D-43F7-A506-A9DA075E229C}
System.Management.Instrumentation.ManagedCommonProvider
{550DDA30-0541-11D2-9CA9-0060B0EC3D39}  XML Data Source Object
{5537E283-B1E7-4EF8-9C6E-7AB0AFE5056D}  CRasProvider
{555F3418-D99E-4E51-800A-6E89CFD8B1D7}  HWDeviceCustomProperties
{5569e7f5-424b-4b93-89ca-79d17924689a}  Windows Media Player Plug-in Registrar
{559C6BAD-1EA8-4963-A087-8A6810F9218B}  CThumbnailGeneratorDmo
{55B3A0BD-4D28-42fe-8CFB-FA3EDFF969B8}
{55d7b852-f6d1-42f2-aa75-8728a1b2d264}  Size Categorizer
{56198675-BD59-3B10-8346-583781462CEF}
{563DC062-B09A-11D2-A24D-00104BD35090}  WSHController
{566296fe-e0e8-475f-ba9c-a31ad31620b1}
{566A2EFF-5651-4020-AC1A-EB48E4571EA3}  Windows Media SDK HTTP Source Plugin
{5686a0d9-fe39-409f-9dff-3fdbc849f9f5}  Mpeg4s Decoder MFT
{56ad4c5d-b908-4f85-8ff1-7940c29b3bcf}  Window Property Store
{56FDF344-FD6D-11d0-958A-006097C9A090}  Task Bar Communication
{573bdf38-df23-427f-acb8-a67abd702698}  VssModuleKeeper
{5740A302-EF0B-45ce-BF3B-4470A14A8980}  iTV Capture Feature Segment
{57558531-C262-471E-95DB-8B181925C61B}  Infrastructure Setup Page Class
{57635537-C856-4cc2-AE5C-62C34708070C}  Shell Security Zone Checker
{57651662-CE3E-11D0-8D77-00C04FC99D61}  CmdFileIcon
{576C9E85-1300-4EF5-BF6B-D00509F4EDCD}  Sync Center Handler Properties Extension
{577FAA18-4518-445E-8F70-1473F8CF4BA4}  Utility Object for Binding Events
SubObjects in Script Variables
{57C06EAA-8784-11D0-83D4-00A0C911E5DF}  Microsoft Client Configuration Notify
Object
{57f8510b-a5e2-41da-a8f0-8a5ae85dfffd}  Browser Class Factory Creator
{5805137A-E348-4F7C-B3CC-6DB9965A0599}
{5815ADD9-95C5-44F2-8262-3BCD56AA3147}  Windows Search Manager Event Sink
{58221C65-EA27-11CF-ADCF-00AA00A80033}  FILEMGMT 1.0 Object
{58221C66-EA27-11CF-ADCF-00AA00A80033}  SvcVwr 1.0 Object
{58221C69-EA27-11CF-ADCF-00AA00A80033}  FILEMGMT 1.0 Object
{58221C6A-EA27-11CF-ADCF-00AA00A80033}  SvcVwr 1.0 Object
                          Page 68
```

```
                          SOFTWARE OUTPUT.txt
   {5839FCA9-774D-42A1-ACDA-D6A79037F57F}   Microsoft WBEM _WbemFetchRefresherMgr
Proxy Helper
   {58476F97-6464-4e49-9BCB-DD88816A60A3}
   {5848A73D-E9C2-499E-BB92-887CABCB2BD6}   Microsoft XPS Active Document
   {58859c43-2c82-454b-86c0-9efb11e54838}   Ratings Categorizer
   {58AB2366-D597-11d1-B90E-00C04FC9B263}   EapTlsCfg Class
   {58C2B4D0-46E7-11D1-89AC-00A0C9054129}   DirectMusicSynth
   {58E3C745-D971-4081-9034-86E34B30836A}   Speech Recognition
   {58ECEE30-E715-11CF-B0E3-00AA003F000F}   FoxOLEDB 1.0 Object
   {58fb76b9-ac85-4e55-ac04-427593b1d060}   Certificate Services Client Task Handler
   {59031a47-3f72-44a7-89c5-5595fe6b30ee}   UsersFiles
   {59099400-57FF-11CE-BD94-0020AF85B590}   Disk Copy Extension
   {591209c7-767b-42b2-9fba-44ee4615f2c7}   Application Registration
   {593817A0-7DB3-11CF-A2DE-00AA00B93356}   DirectDraw Clipper Object
   {596742A5-1393-4e13-8765-AE1DF71ACAFB}   Microsoft Breadcrumb Bar
   {59699770-2BF1-46C6-857C-1D509DB7079E}   GlobalServiceDS Class
   {597D4FB0-47FD-4aff-89B9-C6CFAE8CF08E}   ManipulationProcessor Class
   {599F9021-5643-4965-9949-E88975EFFF0E}   PSFactoryBuffer
   {59A437AB-74F3-4de2-AFE6-54203634C4DD}   Share Permission List
   {59CE6880-ACF8-11CF-B56E-0080C7C4B68A}   Performance Property Page
   {59DC47A8-116C-11D3-9D8E-00C04F72D980}   BDA Tuning Model Component Class(Broadcast
Substream)
   {5A41EFA3-6C01-43DC-8C49-110151B36C70}   Line 21 Decoder Text Output
   {5A580C11-E5EB-11d1-A86E-0000F8084F96}   CLSID_IHTTPMailTransport
   {5B035261-40F9-11D1-AAEC-00805FC1270E}   Network Configuration Component Object
   {5B18AB61-091D-11D1-97DF-00C04FB9618A}   Microsoft DTC Transaction Manager
   {5b4dae26-b807-11d0-9815-00c04fd91972}   Menu Band
   {5b53b2c2-46d6-433e-ab6e-b82efef22b6e}   ExplorerCommandEnumerator
   {5b858418-cfb4-4b32-8501-54d8b0c59f90}   Item Enumerator Over Categories
   {5BAF654A-5A07-4264-A255-9FF54C7151E7}   UpdateDownloader Class
   {5BF9AA75-D7FF-4aee-AA2C-96810586456D}
   {5C140836-43DE-11d3-847D-00C04F79DBC0}   SCPTRANS Class
   {5C5C1935-0235-4434-80BC-251BC1EC39C6}
   {5C63C1AD-3956-4FF8-8486-40034758315B}   Home Networking Sharing Configuration
Manager
   {5cb66670-d3d4-11cf-acab-00a024a55aef}   COM+ Extended Transaction Context
Component
   {5CDCB131-A1A1-4FE9-9A10-80EFFE042AE0}   video clips container
   {5D08B586-343A-11D0-AD46-00C04FD8FDFF}   Microsoft WBEM Event Subsystem
   {5d1026ee-3f2e-4ccb-a83d-cefb7ac22a71}   Share Media Control Panel
   {5d4d54b3-9fb4-4662-8173-c48568d5e79e}   Percent Categorizer
   {5D6179C8-17EC-11D1-9AA9-00C04FD8FE93}   Microsoft Local Users and Groups MMC
Snap-in
   {5D6179D2-17EC-11D1-9AA9-00C04FD8FE93}   Microsoft Local Users and Groups MMC
Snap-in About Provider
   {5D8E73F7-4989-4ac8-8A98-39BA0D325302}   MSVidCtl Digital TV to iTV Composition
Segment
   {5D9DD151-65F4-11CE-900D-00AA00445589}   Microsoft DTC Transaction Manager Proxy
(private, internal)
   {5DB2625A-54DF-11D0-B6C4-0800091AA605}   ICM Monitor Management
   {5DC41690-C6A6-11d1-9D35-006008B0E5CA}
   {5DC41691-C6A6-11d1-9D35-006008B0E5CA}
   {5DC41692-C6A6-11d1-9D35-006008B0E5CA}
   {5DC41693-C6A6-11d1-9D35-006008B0E5CA}
   {5DC41694-C6A6-11d1-9D35-006008B0E5CA}
   {5E032150-8C1E-4c9e-BC60-36E9BFFCFF56}   HomeGroup Peer Manager
   {5E1395B2-B685-44e3-8AED-E2304D85ACD1}   WiaWow64
   {5E33D52F-2EE2-48EE-80FC-543DFF43E326}   IGD Helper Class
   {5E6AB780-7743-11CF-A12B-00AA004AE837}   Microsoft Internet Toolbar
   {5e941d80-bf96-11cd-b579-08002b30bfeb}   Plain Text persistent handler
   {5ead82c2-28f1-4f7f-956d-d37420b5a687}   Mobile Broadband Connecting Page Class
   {5ef4af3a-f726-11d0-b8a2-00c04fc309a4}   Recycle Bin Cleaner
   {5f4baad0-4d59-4fcd-b213-783ce7a92f22}   WIA Event Prompt Class
                              Page 69
```

SOFTWARE OUTPUT.txt
```
{5F5295E0-429F-1069-A2E2-08002B30309D}  Drive Property Page Extension
{5F5AFF4A-2F7F-4279-88C2-CD88EB39D144}  Microsoft MPEG-2 Encoder
{5FA29220-36A1-40f9-89C6-F4B384B7642E}  Shell Message Handler
{6004c347-d3f3-472a-8f9e-319b5c583d55}  DESC_ItemThumbnail
{60173D16-A550-47f0-A14B-C6F9E4DA0831}  Mount Point Rename
{602BDCE5-CA64-4E91-B27C-FFCA48978A00}  Windows Search Index Notification Sink
{603D3800-BD81-11d0-A3A5-00C04FD706EC}  Background Task Scheduler
{603D3801-BD81-11d0-A3A5-00C04FD706EC}  Shared Task Scheduler
{6047F837-D527-467E-9DC1-6D51F92D9E45}  Wordpad ODT Filter
{60542247-0249-417D-949B-2F0CC7EE1165}  Manual Setup Page Class
{60664caf-af0d-0005-a300-5c7d25ff22a0}  Shell Local Machine Object
{60F6E464-4DEF-11d2-B2D9-00C04F8EEC8C}  Old Files In Root Prop Bag
{60F6E465-4DEF-11d2-B2D9-00C04F8EEC8C}  Temp Files Prop Bag
{60F6E466-4DEF-11d2-B2D9-00C04F8EEC8C}  Setup Files Prop Bag
{60F6E467-4DEF-11d2-B2D9-00C04F8EEC8C}  Uninstall Prop Bag
{60fd46de-f830-4894-a628-6fa81bc0190d}  DropTarget Object for Photo Printing
Wizard
{6131A8EC-78CE-11d2-A3F2-3078302C2030}
{61b68808-8eee-4fd1-acb8-3d804c8db056}  Contact class
{61E79517-4A4E-45D8-9219-30E71A9EFF39}  TabletButtonExtendedActions Class
{61F7B364-432C-4D04-BBC1-7FC1BF3807A8}  Bluetooth Bluewire Shell property
extension object
{61FFC721-B206-45d0-B02E-6AA7E52E1575}  DictationHost Class
{62079164-233b-41f8-a80f-f01705f514a8}  EVR Graph Optimizer
{62112AA1-EBE4-11cf-A5FB-0020AFE7292D}  Shell Automation Folder View
{622a8646-1096-4765-8e07-91a3e661cef9}  XWizard Factory Generated Class (HomeGroup
Leave Hook Page)
{622D47B6-CEEC-4DE1-8056-B6D16F29BC97}  Microsoft WBEM Rpc Message Sender
{626BAFE6-E5D6-11D1-B1DD-006097D503D9}  CLSID_OERulesManager
{6276916E-8F41-35C7-B1D2-1D289A63BE7C}
{6295DF27-35EE-11D1-8707-00C04FD93327}  Sync Manager (Legacy)
{6295DF2D-35EE-11D1-8707-00C04FD93327}  Sync Center (Private)
{62AE1F9A-126A-11D0-A14B-0800361B1103}
{62BE5D10-60EB-11d0-BD3B-00A0C911CE86}  System Device Enumerator
{62CE7E72-4C71-4D20-B15D-452831A87D9D}  Microsoft H264 Video Decoder MFT
{6311429E-2F1A-4777-880F-C7289FD10169}  Inplace Share Engine
{632A2D3D-86AF-411A-8654-7511B51B3D5F}  Lattice Class
{636B9F10-0C7D-11D1-95B2-0020AFDC7421}  DirectMusic
{636c15cf-df63-4790-866a-117163d10a46}  MFRemoteDesktopPlugin Class
{639F5AF5-BCED-4369-AC34-360B16D955FD}  GestureRecognizer Class
{63A865AB-859E-4f15-8AEC-77FC615653D9}  WMPlayer FileFormatPropPage Class
{63B51F81-C868-11D0-999C-00C04FD655E1}  Shell Icon Overlay Manager
{63FA5E69-87FE-432d-8F62-9D7A3D7D09C3}  WMPlayer VideoPerfPropPage Class
{6438570B-0C08-4A25-9504-8012BB4D50CF}  Tuner Marshaling Helper
{64577982-86D7-11d1-BDFC-00C04FA31009}  CLSID_IHashTable
{645FF040-5081-101B-9F08-00AA002F954E}  Recycle Bin
{64818D10-4F9B-11CF-86EA-00AA00B929E8}
{64818D11-4F9B-11CF-86EA-00AA00B929E8}
{649c5690-507e-494a-9e89-1eb24e4bce3d}  WMPMDE LPCM SINK ACTIVATE
{64B8F404-A4AE-11D1-B7B6-00C04FB926AF}  PSFactoryBuffer
{64BC32B5-4EEC-4de7-972D-BD8BD0324537}  Search Control
{64D8A8E0-80A2-11d2-8CF3-00A0C9441E20}  RenderEngine Class
{6504AFED-A629-455C-A7F1-04964DEA5CC4}  BDA Tuning Model ISDB Satellite Locator
{650503CF-9108-4DDC-A2CE-6C2341E1C582}  WebProxy Class
{6522CF99-94C7-4958-B18D-4F6159E6926B}  Policy for DWM items tree item callback
object for sysdm.cpl
{65303443-AD66-11D1-9D65-00C04FC30DF6}  OleCvt Class
{6543D242-A80B-44A3-B828-95C1EC452423}  ActualWbemAuthenticatedLocator Class
{659cdea7-489e-11d9-a9cd-000d56965251}  Background Intelligent Transfer Control
Class 3.0
{65BD0711-24D2-4FF7-9324-ED2E5D3ABAFA}  MediaDet
{65d00646-cde3-4a88-9163-6769f0f1a97d}  InkOverlay Class
{660b90c8-73a9-4b58-8cae-355b7f55341b}  Start Menu Cache
```
Page 70

SOFTWARE OUTPUT.txt

```
{661FF7F6-F4D1-4593-B59D-4C54C1ECE68B}    WmiPerf Class Provider
{66275315-bfa5-451b-88b6-e56ebc8d9b58}    Library Property Handler
{662C0206-72AD-4ee9-899F-5E1735F60A55}    WMPDMCMedia Class
{66742402-F9B9-11D1-A202-0000F81FEDEE}
{66d56b60-97b7-4e6a-9aa1-3ec5e3fdaa0f}    Winsock Diagnostic Helper Class
{66e4e4fb-f385-4dd0-8d74-a2efd1bc6178}    Shell Image Data Factory
{66EC5C50-45B7-48cd-81D6-20A712011AD1}    SpeechUXHost Class
{66eea0f5-001a-4073-a496-783f86fcf4c0}    Windows Data Burn
{6705C562-0AE7-40EA-8474-F39DAB1813D0}    RAS Media Manager
{6746c347-576b-4f73-9012-cdfeea251bc4}    CLSID_ScopeFactory
{674B6698-EE92-11D0-AD71-00C04FD8FDFF}    Microsoft WBEM Call Context
{6756A641-DE71-11d0-831B-00AA005B4383}    MRU AutoComplete List
{675F097E-4C4D-11D0-B6C1-0800091AA605}    ICM Printer Management
{67718415-c450-4f3c-bf8a-b487642dc39b}    Windows Features
{6785BFAC-9D2D-4be5-B7E2-59937E8FB80A}    Other Users Folder
{67CA7650-96E6-4FDD-BB43-A8E774F73A57}    HomeGroup Control Panel
{67F07E00-CCEF-11D2-9EF9-006008039E37}    Audio Mixer Property
{681FD532-7EC2-4548-9ECE-44AABCFBD254}    Registry Provider Class
{682159d9-c321-47ca-b3f1-30e36b2ec8b9}    CLSID_DesktopExplorerHost
{687607A0-6BA1-4355-99F4-4E3D749FFB19}    WlanDlgOneXUIPage Class
{687D3367-3644-467a-ADFE-6CD7A85C4A2C}    MPEG-2 Demultiplexer(NoClock)
{687e55ca-6621-4c41-b9f1-c0eddc94bb05}    SdController Class
{68b07bff-cb50-4d60-a7d5-02b1a523bc8c}    SearchConnector Icon Extract Extension
{68B67DA9-7212-396E-9528-33F70547660E}
{68c67565-410e-45e6-8560-4091ae193481}
{68E3F2FD-31AE-4441-BB6A-FD7047525F90}
{68e52c1c-37cb-41d2-afe1-1e77d5f10676}    Autoplay Device Event Handler Info
{69127644-2511-4DF5-BC6A-26178254AA40}    RemoteAssistance Class
{6935DB93-21E8-4ccc-BEB9-9FE3C77A297A}    Custom MRU AutoCompleted List
{693644B0-6858-11D2-9EEB-006008039E37}    Still Video Property Page
{69546697-5b53-43c5-8391-9e227b54957b}    IARPUninstallerProxy
{698A4FFC-63A3-4E70-8F00-376AD29363FB}    Wordpad OOXML Document Filter
{699745C2-5066-4B82-A8E3-D40478DBEC8C}
{69AD4AEE-51BE-439b-A92C-86AE490E8B30}    Legacy Background Intelligent Transfer
Control Class
{69B37063-2BB6-43b5-A109-60E69A77840F}    WcsPlugInService Class
{69BE8BB4-D66D-47C8-865A-ED1589433782}
{69F9CB25-25E2-4BE1-AB8F-07AA7CB535E8}    Sync Center Isolation Collection (Private)
{6A08CF80-0E18-11CF-A24D-0020AFD79767}    ACM Wrapper
{6A205B57-2567-4a2c-B881-F787FAB579A3}    Microsoft DocProp Inplace Calendar Control
{6A2A9381-5A92-4296-9397-564673AE1FDD}    CLSID_HomeGroupListenerNotify
{6A2E0670-28E4-11D0-A18C-00A0C9118956}    IAMVideoControl
{6A68CC80-4337-4dbc-BD27-FBFB1053820B}    CSearchLanguageSupport Class
{6AD28EE1-5002-4E71-AAF7-BD077907B1A4}    MSVidCtl MPEG2 Decoder to Closed
Captioning Composition Segment
{6AFCCE9E-85F0-475C-944E-9357B84A4975}    Infrastructure Error Page Class
{6B13B293-30FD-4abb-8E41-29B1F88297E2}    Windows Media Player OCXGeneralPropPage
Class
{6B2D6BA0-9F3E-4f27-920B-313CC426A39E}    Open Packaging API Factory Object
{6b33163c-76a5-4b6c-bf21-45de9cd503a1}    Shell Publishing Wizard Object
{6B362280-6915-11D2-951F-0060081840BC}    Silence Generator Property Page
{6B462062-7CBF-400D-9FDB-813DD10F2778}
{6B6F9D2D-6D49-4026-83A6-86DFC1C3C6F0}    INI Property Set Storage Handler
{6B750899-F157-47D7-9C08-257E7A35141D}
{6B831E4F-A50D-45FC-842F-16CE27595359}    Storage Processor Default Confirmation UI
{6B9228DA-9C15-419e-856C-19E768A13BDC}    Windows Desktop Gadgets
{6BC096B1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B3-0CE6-11D1-BAAE-00C04FC2E20D}    IAS Pipeline
{6BC096B7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096BC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096D5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DA-0CE6-11D1-BAAE-00C04FC2E20D}
```

Page 71

SOFTWARE OUTPUT.txt

```
{6BC096DB-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DE-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DF-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E0-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E2-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E3-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E4-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09894-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09896-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09897-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09898-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09899-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989A-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989B-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989C-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989D-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989E-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989F-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A4-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A6-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A9-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC1CFFA-8FC1-4261-AC22-CFB4CC38DB50}   Default Video Renderer
{6BF0A714-3C18-430b-8B5D-83B1C234D3DB}   PSFactoryBuffer
{6BF52A52-394A-11d3-B153-00C04F79FAA6}   Windows Media Player
{6c19be35-7500-11d1-ad94-00c04fd8fdff}   Microsoft WBEM Event filter marshaling
proxy
{6C5CFCDA-1F1A-4c9e-8D65-94771169D0B9}   GameDetails Class
{6ca50344-051a-4ded-9779-a43305165e35}
{6CF48EF8-44CD-45d2-8832-A16EA016311B}
{6CFAD761-735D-4AA5-8AFC-AF91A7D61EBA}   Mpeg-2 Video Stream Analysis
{6d18ad12-bde3-4393-b311-099c346e6df9}   Background Intelligent Transfer Control
Class 2.0
{6D3951EB-0B07-4fb8-B703-7C5CEE0DB578}   Advanced Indexing Options Dialog Object
{6D5313C0-8C62-11D1-B2CD-006097DF8C11}   Folder Options Property Page Extension
{6D75C88D-82A0-3994-A751-3B82F490D22C}
{6D8BB3D3-9D87-4a91-AB56-4F30CFFEFE9F}   Explorer Search Band
{6d8ff8d2-730d-11d4-bf42-00b0d0118b56}   UPnPEventingManager
{6d8ff8dc-730d-11d4-bf42-00b0d0118b56}   UPnPDynamicContentSource
{6d8ff8dd-730d-11d4-bf42-00b0d0118b56}   UPnPDescriptionManager
{6d8ff8df-730d-11d4-bf42-00b0d0118b56}   UPnPDevicePersistenceManager
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56}   UPnPContainer
{6d8ff8e1-730d-11d4-bf42-00b0d0118b56}   UPnPContainerManager
{6d8ff8e5-730d-11d4-bf42-00b0d0118b56}   UPnPValidationManager
{6d8ff8e7-730d-11d4-bf42-00b0d0118b56}   UPnPContainerManager64
{6d8ff8e8-730d-11d4-bf42-00b0d0118b56}   UPnPContainer64
{6DA736C9-DCDE-4651-82A8-56E4EF1D8DD7}   CLSID_ScfFileExecute
{6DAF9757-2E37-11D2-AEC9-00C04FB68820}   MOF Compiler
{6db29a9b-10d0-4b93-b86a-188fc998eff8}   InfraCreateTask
{6DFD7C5C-2451-11d3-A299-00C04F8EF6AF}   Folder Options
{6e18f9c6-a3eb-495a-89b7-956482e19f7a}   WinSAT Accessibility Object
{6e29fabf-9977-42d1-8d0e-ca7e61ad87e6}   UIAutomation Registrar Class
{6e33091c-d2f8-4740-b55e-2e11d1477a2c}   Shell Image Recompression Object
{6E3D2E94-E6D8-4afd-AFDE-ABD26CA88BF5}   FaultrepDataCollectionInProc
{6E4FCB12-510A-4d40-9304-1DA10AE9147C}   InkTablets Class
```

Page 72

```
                         SOFTWARE OUTPUT.txt
 {6e682784-1eca-4cf2-988d-96b6e89e9a4d}  CLSID_SearchIDListFactory
 {6E78DAD9-E187-4D6E-BA63-760256D6F405}  Microsoft Session And Connection Provider
 {6EB22881-8A19-11D0-81B6-00A0C9231C29}  Catalog Class
 {6EDD6D74-C007-4E75-B76A-E5740995E24C}  PSFactoryBuffer
 {6EF07F29-F9B8-4DA4-B59E-13DEA060AD60}
 {6efeae9e-014c-436a-8aac-35da9535adc0}  Windows Media Player InputCollection Class
 {6F26A6CD-967B-47FD-874A-7AED2C9D25A2}  Video Port Manager
 {6f33340d-8a01-473a-b75f-ded88c8360ce}  HomeGroup UI Status
 {6f45dc1e-5384-457a-bc13-2cd81b0d28ed}  PasswordProvider
 {6F74FDC5-E366-11d1-9A4E-00C04FA309D4}  CLSID_MessageDatabase
 {6F74FDC6-E366-11d1-9A4E-00C04FA309D4}  CLSID_FolderDatabase
 {6F7C8E8F-DC69-4e3f-BC05-439962A05FD5}  CLSID_HomeGroupProvider
 {6F8DAE82-43A2-47AA-B0E7-47B7E82F705F}  WMEncSourcePluginWrapper
 {6FE54E0E-009F-4E3D-A830-EDFA71E1F306}  Bluetooth Personal Area Connection
 {7007ACC1-3202-11D1-AAD2-00805FC1270E}  Dial-up Connection UI Class
 {7007ACC3-3202-11D1-AAD2-00805FC1270E}  Inbound Connection UI Class
 {7007ACC4-3202-11D1-AAD2-00805FC1270E}  Internet Connection UI Class
 {7007ACC5-3202-11D1-AAD2-00805FC1270E}  LAN Connection UI Class
 {7007ACC6-3202-11D1-AAD2-00805FC1270E}  VPN Connection UI Class
 {7007ACC7-3202-11D1-AAD2-00805FC1270E}  Network Connections
 {7007ACC8-3202-11D1-AAD2-00805FC1270E}  Network Connections Enum
 {7007ACCF-3202-11D1-AAD2-00805FC1270E}  Network Connections Tray
 {7007ACD1-3202-11D1-AAD2-00805FC1270E}  Network Common Connections Ui
 {7007ACD3-3202-11D1-AAD2-00805FC1270E}  Net Connections UI Utilities Class
 {7007ACD4-3202-11D1-AAD2-00805FC1270E}  PPPoE UI Class
 {7007ACD5-3202-11D1-AAD2-00805FC1270E}  Shared Access Connection UI Class
 {7016F8FA-CCDA-11D2-B35C-00105A1F8177}  Microsoft WBEM (non)Standard Marshaling
for IWbemMultiTarget
 {7071EC01-663B-4bc1-A1FA-B97F3B917C55}  Build Connections Options Page Class
 {7071EC05-663B-4bc1-A1FA-B97F3B917C55}  Display Connection Options Page Class
 {7071EC07-663B-4bc1-A1FA-B97F3B917C55}  Handle Diagnostics Page Class
 {7071EC13-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Connect To Internet Page
Class
 {7071EC31-663B-4bc1-A1FA-B97F3B917C55}  ISP Offer Page Class
 {7071EC32-663B-4bc1-A1FA-B97F3B917C55}  ISP Confirm Page Class
 {7071EC33-663B-4bc1-A1FA-B97F3B917C55}  ISP CD Page Class
 {7071EC61-663B-4bc1-A1FA-B97F3B917C55}  Display Internet Existing Connections Page
Class
 {7071EC62-663B-4bc1-A1FA-B97F3B917C55}  Display Work Existing Connections Page
Class
 {7071EC71-663B-4bc1-A1FA-B97F3B917C55}  Create Dial-up Task Class
 {7071EC75-663B-4bc1-A1FA-B97F3B917C55}  Create VPN Task Class
 {7071EC77-663B-4BC1-A1FA-B97F3B917C55}  XWizard Factory Generated Class
 {7071ECA0-663B-4bc1-A1FA-B97F3B917C55}  Connect To Internet Task Class
 {7071ECA3-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Detection Hook
Page Class
 {7071ECA5-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Creation Hook Page
Class
 {7071ECA7-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Testing Hook Page
Class
 {7071ECA8-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Hook Page Class
 {7071ECA9-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Diagnostics Hook
Page Class
 {7071ECAF-663B-4bc1-A1FA-B97F3B917C55}  Connect To The Internet Finish Page Class
 {7071ECB0-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Task Class
 {7071ECB3-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Detection Hook Page Class
 {7071ECB4-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Existing Connections Page
Class
 {7071ECB5-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Creation Hook Page Class
 {7071ECB6-663B-4BC1-A1FA-B97F3B917C55}  XWizard Factory Generated Class
 {7071ECB7-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Testing Hook Page Class
 {7071ECB8-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Hook Page Class
 {7071ECBF-663B-4bc1-A1FA-B97F3B917C55}  Connect To Work Finish Page Class
                              Page 73
```

SOFTWARE OUTPUT.txt

```
{7071ECD0-663B-4bc1-A1FA-B97F3B917C55}  Connect To Bluetooth Task Class
{7071ECD5-663B-4bc1-A1FA-B97F3B917C55}  Display Bluetooth Adapters Page Class
{7071ECE0-663B-4bc1-A1FA-B97F3B917C55}  Connect To Network Task Class
{7071ECE5-663B-4bc1-A1FA-B97F3B917C55}  Connect To Network Page Class
{7071ECF1-663B-4bc1-A1FA-B97F3B917C55}  Message Page Class
{7071ECFA-663B-4bc1-A1FA-B97F3B917C55}  Network Tasks Host Class
{70804ECC-7272-4dc8-AFFC-97CD66AAA282}  Windows Desktop Search Map Plugin
{7098BB2E-EB80-4433-BEF6-DF45206A41DC}  Vista Share Engine
{709E2729-F883-441e-A877-ED3CEFC975E6}  ProfileNotifyHandler Class
{70cba7d2-50a5-4383-8aa5-b378c01c7364}  CLSID_LegacyFindFiles
{70E102B0-5556-11CE-97C0-00AA0055595A}  Video Renderer
{70f598e9-f4ab-495a-99e2-a7c4d3d89abf}  WMAudio Encoder DMO
{70f98452-3c38-4271-8e76-6f444852ebc8}  PortableDeviceWiaCompat Class
{70FF37C0-F39A-4B26-AE5E-638EF296D490}  RARegSetting Class
{7122A82D-E722-4AFC-AA87-EAA77D8CFCE1}  Windows Media Player WMEnc5PointWavSource
Class
{71285C44-1DC0-11D2-B5FB-00104B703EFD}  Microsoft WBEM (non)Standard Marshaling
for IWbemObjectSink
{713790EE-5EE1-45ba-8070-A1337D2762FA}  WTVFile Thumbnail Handler
{713aacc8-3b71-435c-a3a1-be4e53621ab1}  AnimateWindowSize Object
{7165c8ab-af88-42bd-86fd-5310b4285a02}  ContactManager class
{717ef4fe-ac8d-11d0-b945-00c04fd8d5b0}  DsPropertyPages.User Special Info
{71932D43-3CA5-46EF-B013-3F9A695996ED}  DMO Wrapper Filter
{71985F4B-1CA1-11D3-9CC8-00C04F7971E0}
{71D99464-3B6B-475C-B241-E15883207529}  Sync Results Folder
{71E32BAA-73EE-40a1-933C-F166F0192B72}  Show thumbnails instead of icons tree item
callback object for sysdm.cpl
{71E38F91-7E88-11CF-9EDE-0080C78B7F89}  MTxAS Object
{71f96385-ddd6-48d3-a0c1-ae06e8b055fb}  Explorer Browser
{71F96460-78F3-11d0-A18C-00A0C9118956}  %Filter_XBar%
{71F96461-78F3-11d0-A18C-00A0C9118956}  Analog Crossbar Property Page
{71F96462-78F3-11d0-A18C-00A0C9118956}  WDM TV Audio
{71F96463-78F3-11d0-A18C-00A0C9118956}  TV Audio Property Page
{71F96464-78F3-11D0-A18C-00A0C9118956}  VideoProcAmp Property Page
{71F96465-78F3-11D0-A18C-00A0C9118956}  CameraControl Property Page
{71F96466-78F3-11D0-A18C-00A0C9118956}  VideoDecoder Property Page
{71F96467-78F3-11D0-A18C-00A0C9118956}  VideoStreamConfig Property Page
{720D4AC0-7533-11D0-A5D6-28DB04C10000}  KsTopologyInfo Class
{722b3793-5367-4446-b6bb-db89b05c1f24}  ItemHandlerCache
{725F645B-EAED-4fc5-B1C5-D9AD0ACCBA5E}  File Open Dialog Legacy
{728a21c5-3d9e-48d7-9810-864848f0f404}  PortableDevice Class
{72A7994A-3092-4054-B6BE-08FF81AEEFFC}  Sharing Elevated Virtual Factory
{72b36e70-8700-42d6-a7f7-c9ab3323ee51}  Search Connector Folder
{72C24DD5-D70A-438B-8A42-98424B88AFB8}  Windows Script Host Shell Object
{72c57034-02c4-4e9f-bf9c-ca711031757e}  Shell File Operation Undo Unit
{72C97D74-7C3B-40AE-B77D-ABDB22EBA6FB}  StringCollection Class
{72d3edc2-a4c4-11d0-8533-00c04fd8d503}  ADs Property Entry Object
{72eb61e0-8672-4303-9175-f2e4c68b2e7c}  Namespace Walker
{73647561-0000-0010-8000-00AA00389B71}  WDM Streaming Standard Data Type Handler
{73C037E7-E5D9-4954-876A-6DA81D6E5768}
{73D14237-B9DB-4efa-A6DD-84350421FB2F}  MSVidCtl Digital TV to CCA Composition
Segment
{73DA5D04-4347-45D3-A9DC-FAE9DDBE558D}  CSectionList
{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}  Microsoft WMI Provider Subsystem Host
{740EC24D-46AD-4334-A076-41CCC3F8D9B4}  PBDA Class
{74246bfc-4c96-11d0-abef-0020af6b0b7a}  Device Manager
{743a6e3b-a5df-43ed-b615-4256add790b8}  MFPsiFilter
{7447A267-0015-42C8-A8F1-FB3B94C68361}
{745057c7-f353-4f2d-a7ee-58434477730e}  AEC
{745a5add-6a71-47b9-9bb9-31dd3a6913d4}  Authentication UI CredUI Helper
{7469AE5E-1CA1-4181-970C-BDFD8EAA2C4F}  PSFactoryBuffer
{74807f67-0058-440d-8600-65541a7fbbea}  PSFactoryBuffer
{7487cd30-f71a-11d0-9ea7-00805f714772}  Background Thumbnail Generator
```

Page 74

SOFTWARE OUTPUT.txt
```
{75048700-EF1F-11D0-9888-006097DEACF9}   ActiveDesktop
{7542E960-79C7-11D1-88F9-0080C7D771BF}   Event Subscription
{75847177-f077-4171-bd2c-a6bb2164fbd0}   Private Profile Object
{75C9378A-7E89-11d2-B116-00805FC73204}
{75dff2b7-6936-4c06-a8bb-676a7b00b24b}   CLSID_SeparateMultipleProcessExplorerHost
{760C4B83-E211-11D2-BF3E-00805FBE84A6}   Windows Media Services DRM Storage object
{7669CAD6-BDEC-11D1-A6A0-00C04FB9988E}   ProtocolsTable Class
{76765b11-3f95-4af2-ac9d-ea55d8994f1a}   Property System Both Class Factory
{76B4FCAC-BB29-11DB-96F1-005056C00008}   PBDA ETFilter
{76be8257-c4c0-4d37-90c0-a23372254d27}   Indexer Status Update Object
{76D0CB12-7604-4048-B83C-1005C7DDC503}
{76f014ec-1b0c-4a15-a029-4c0fdf12b5b1}   Briefcase Storage Object
{7751F46E-39B2-4b50-A7E3-23EF598ECD85}   Selector Class
{77597368-7B15-11D0-A0C2-080036AF3F03}   PrintUIShellExtension Class
{7763B7C0-A5FD-4AA9-BD1B-58B17137236B}   Location Description
{777BA815-2498-4875-933A-3067DE883070}   XWizard Task Stub
{777BA816-2498-4875-933A-3067DE883070}   XWizard Page Stub
{777BA81A-2498-4875-933A-3067DE883070}   XWizard Virtual Factory
{777BA851-2498-4875-933A-3067DE883070}   XWizard Type plugin for Win32 Class
{777BA853-2498-4875-933A-3067DE883070}   XWizard Type plugin for DUI Class
{777BA87C-2498-4875-933A-3067DE883070}   Public XWizard Manager Class
{777BA8D2-2498-4875-933A-3067DE883070}   Public Simple Marshal Class
{777BA8E3-2498-4875-933A-3067DE883070}   Private XWizard Page Enumeration Manager
Class
{777BA8E5-2498-4875-933A-3067DE883070}   Private XWizard Task Enumeration Manager
Class
{777BA8E7-2498-4875-933A-3067DE883070}   Private XWizard Host Enumeration Manager
Class
{777BA8E9-2498-4875-933A-3067DE883070}   Private XWizard Registry Information
Manager Class
{777BA8F5-2498-4875-933A-3067DE883070}   Private XWizard Registration Manager Class
{777BA8F9-2498-4875-933A-3067DE883070}   Private XWizard Factory Registration
Manager Class
{777BA8FB-2498-4875-933A-3067DE883070}   Private XWizard Type Registration Manager
Class
{777D0CFF-0375-43b9-8532-FB04A4903593}   Windows Media Player Effects Activate
{77F10CF0-3DB5-4966-B520-B7C54FD35ED6}   Custom Destination List
{77F419AA-771A-45ff-AC66-7567FA3243D3}   SMB Share Engine
{77F7F122-20B0-4117-A2FB-059D1FC88256}   WPDServiceProvider Class
{780102B0-C43B-4876-BC7B-5E9BA5C88794}   PSFactoryBuffer
{78103FB7-AED7-4066-8BCD-30BB27B02331}   Microsoft WBEM WMI Object Factory
{782fc20a-81cf-43de-a625-072155bcd30c}   XWizard Factory Generated Class (HomeGroup
Create Hook Page)
{784215B4-0D2E-11D3-920A-00C0DF10D434}   MediaDetFilter
{7849596a-48ea-486e-8937-a2a3009f31a9}   PostBootReminder object
{78530B75-61F9-11D2-8CAD-00A024580902}   MS Timeline
{786CDB70-1628-44A0-853C-5D340A499137}   TabletManager Class
{7886B467-66D4-4163-82BA-D9212FDB4CA8}   Windows Security Health Agent Callback
Component
{7888E5FE-6C66-4A34-B217-FA2292073F4A}   PSFactoryBuffer
{78F3955E-3B90-4184-BD14-5397C15F1EFC}   Performance Information and Tools
{78fe669a-186e-4108-96e9-77b586c1332f}   Content Index Null Stemmer
{79376820-07D0-11CF-A24D-0020AFD79767}   DirectSound Audio Renderer
{797A9BB1-9E49-4e63-AFE1-1B45B9DC8162}   DeviceHostICSSupport Class
{798059F0-89CA-4160-B325-AEB48EFE4F9A}   CColorControlDmo
{7986d495-ce42-4926-8afc-26dfa299cadb}   Authentication UI Logon UI
{7998DC37-D3FE-487C-A60A-7701FCC70CC6}   Microsoft WBEM A51 Repository
{7999FC25-D3C6-11CF-ACAB-00A024A55AEF}   COM+ Transaction Context Component
{79eac9d0-baf9-11ce-8c82-00aa004ba90b}   StdHlink
{79eac9d1-baf9-11ce-8c82-00aa004ba90b}   StdHlinkBrowseContext
{7A0CC021-2939-4379-AA82-12AECC3538F6}   CLSID_INewsgroupHelp
{7A0F6AB7-ED84-46B6-B47E-02AA159A152B}   Simple Conflict Presenter
{7A56C4CB-D678-4188-85A8-BA2EF68FA10D}   SAMI Byte Stream Handler
```
Page 75

SOFTWARE OUTPUT.txt

```
{7A7C3277-8F84-4636-95B2-EBB5507FF77E}  LatLongReport Class
{7A80E4A8-8005-11D2-BCF8-00C04F72C717}  ExtractIcon Class
{7A9D77BD-5403-11d2-8785-2E0420524153}  User Accounts
{7aa7790d-75d7-484b-98a1-3913d022091d}  Shell FMIFS Wrapper
{7abbbcca-e01b-4560-8228-92e1eedbc908}  CLSID_CopyUndoHandler
{7AD84985-87B4-4a16-BE58-8B72A5B390F7}  PlayTo
{7AFA253E-F823-42f6-A5D9-714BDE467412}  AVI Byte Stream Handler
{7B19A919-A9D6-49E5-BD45-02C34E4E4CD5}
{7B2801E6-0BC6-4c92-B742-6BE9B01AE874}  DllHostInitializer
{7B31547E-EF7E-479b-9494-2216DC179E61}  Autoplay Handler
{7B3BC2A0-AA50-4ae7-BD44-B03649EC87C2}  VPS Decoder
{7b4a83b6-f704-4b77-8e3d-c6087e3a21d2}  Share Command State Handler
{7B5A12E8-0C60-4939-A046-11CF879B19FB}  WlanDlg Get Key Task Class
{7b81be6a-ce2b-4676-a29e-eb907a5126c5}  Programs and Features
{7b9e38b0-a97c-11d0-8534-00c04fd8d503}  ADs Property Value Object
{7BA4C740-9E81-11CF-99D3-00AA004AE837}  Microsoft SendTo Service
{7bafb3b1-d8f4-4279-9253-27da423108de}  WMV Screen decoder DMO
{7be73787-ce71-4b33-b4c8-00d32b54bea8}  HomeGroup Password
{7be9d83c-a729-4d97-b5a7-1b7313c39e0a}  Programs Folder
{7C07E0D0-4418-11D2-9212-00C04FBBBFB3}  MSPersist
{7C23220E-55BB-11D3-8B16-00C04FB6BD3D}  WM ASF Writer
{7c61d0a6-af7e-483a-b705-d2c5c2264656}  CLSID_EverywhereScopeFiller
{7C857801-7381-11CF-884D-00AA004B2E24}  PSFactoryBuffer
{7CB359C5-570F-43c6-971F-1DB499EE57A1}  WMPlayer PlaybackPropPage Class
{7cd3c903-d2e9-4a4d-8af3-3025445b24bf}  FilterControl
{7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}  Windows Search Manager
{7d13f939-b90e-42ea-8fb6-c2183f14c578}  Redo command invocation
{7D22E920-5CA9-4787-8C2B-A6779BD11781}
{7D3195FF-A16A-43c3-9E50-E8A0975B234C}  BTHPAN Device Center Context Menu Handler
{7D8AA343-6E63-4663-BE90-6B80F66540A3}  VMR ImageSync
{7D9239E5-782C-4126-99AD-81F0E8DA8F5C}  New Network category Options Page
{7d9ad905-b754-4297-b2eb-8371abe25540}  Adhoc Networks Exists Page
{7DB7A939-E5C8-4eaa-B3E0-43CE04CAFFBE}
{7df2cfcd-6c09-415a-ae9d-5263f4964cbb}  CLSID_SortColumnArray
{7DF62B50-6843-11D2-9EEB-006008039E37}  Generate Still Video
{7DF8EF76-D449-485f-B4EB-58DC96B31EDB}  HomeGroup Printing Device Class
{7e320092-596a-41b2-bbeb-175d10504eb6}  WMVideo8 Encoder DMO
{7E37D5E7-263D-45CF-842B-96A95C63E46C}  Group Policy Object Proxy Stub
{7E3FCEA1-31B4-11D2-AE1F-0080C7337EA1}  XML Viewer Moniker
{7E4A23E2-B969-4761-BE35-1A8CED58E323}  XPS Thumbnail Generator
{7E66DBEF-2474-4E82-919B-9A855F4C2FE8}  WscIsvIf Proxy Stub
{7e99c0a3-f935-11d2-ba96-00c04fb6d0d1}  ADs DN With Binary Object
{7E9D8D44-6926-426F-AA2B-217A819A5CCE}  XML File Persistent Handler
{7EB5FBE4-2100-49E6-8593-17E130122F91}  Fade Task
{7F1899DA-62A6-11D0-A2C6-00C04FD909DD}  ScopeTree 1.0 Object
{7F368827-9516-11D0-83D9-00A0C911E5DF}  Microsoft Server Configuration Notify
Object
{7F43B400-1A0E-4D57-BBC9-6B0C65F7A889}  PSFactoryBuffer
{7F598975-37E0-4A67-A992-116680F0CEDA}  Microsoft WMI Provider Subsystem Self
Instrumentation
{7f5d25f8-78a5-49a8-a33c-2c0e11831c66}  WMDRM Context
{7F72CC7A-74A0-45B4-909C-14FB8186DD7E}  WBEM IP DFS Provider
{7F73B8F6-C19C-11D0-AA66-00C04FC2EDDC}
{7f8e7858-c362-4c0a-b868-4cdd929da715}  Authentication UI User Settings
{7F9CB14D-48E4-43B6-9346-1AEBC39C64D3}  MS Video Control Closed Captioning Feature
Segment
{7FE0D935-DDA6-443F-85D0-1CFB58FE41DD}  PSFactoryBuffer
{7febaf7c-18cf-11d2-993f-00a0c91f3880}  DefView Persistent history
{80009818-f38f-4af1-87b5-eadab9433e58}  MF ADTS Property Handler
{804c8e4a-3dae-460d-90ad-8694b510f851}  Microsoft IME IMEPad Server
{807553E6-5146-11D5-A672-00B0D022E945}
{8078DA75-F43F-341D-A00E-20D6D736415E}
{8082C5E6-4C27-48ec-A809-B8E1122E8F97}  .contact shell extension handler
```

Page 76

SOFTWARE OUTPUT.txt

```
{8086ebd4-43e3-4b19-beb3-f0ea4ecf319c}    CScriptedDiagNativeHost
{809B6661-94C4-49E6-B6EC-3F0F862215AA}    Collection of BDA Tuning Model
Components(Broadcast Substreams)
{80c68d96-366b-11dc-9eaa-00161718cf63}    Play command invocation
{80F3F1D5-FECA-45F3-BC32-752C152E456E}    Tablet PC Settings Control Panel
{80F94176-FCCC-11D2-B991-00C04F8ECD78}    MessageView Class
{81007291-f070-4c4f-b978-ad1bec84babc}    Rename command invocation
{8144B6F5-20A8-444a-B8EE-19DF0BB84BDB}    StiEventHandler Class
{814B9800-1C88-11D1-BAD9-00609744111A}    VBI Surface Allocator
{814B9801-1C88-11D1-BAD9-00609744111A}    VideoPort VBI Object
{81796171-DF5F-4F1B-A80C-BE4715D3C6BB}    TextNormMultiResult Class
{819469D2-D0CF-11d1-8E0B-00C04FC2E0C7}
{819d1334-9d74-4254-9ac8-dc745ebc5386}    InfoBar Manager
{81b43e73-e814-4dcd-a7c6-e22e7fe6a029}    Item Store Object
{81BD8EE8-F713-36A5-B7D5-9E92ACB4A18A}
{81E9DD62-78D5-11D2-B47E-006097B3391B}    DVcrControl Property Page
{820825FD-1358-4705-8FEB-56B5CEE8BFD5}    NULL SSID INFO PAGE      (
{823535A0-0318-11D3-9D8E-00C04F72D980}    BDA Tuning Model Component Type Class
(Broadcast Substream Type)
{823B8267-735C-477E-8151-0FA9ADC8AB3A}    Convert ACL to SIDs and resolve SIDs
{82435bdf-f7c1-4df9-8103-eeabebf3d6e1}    WMDRM Content Enabler
{8278F931-2A3E-11d2-838F-00C04FD918D0}    Tracking Shell Menu
{82BD0E67-9FEA-4748-8672-D5EFE5B779B0}
{82c588e7-e54b-408c-9f8c-6af9adf6f1e9}    FormatForDisplay Helper
{82d353df-90bd-4382-8bc2-3f6192b76e34}    WMVideo Decoder DMO
{82d792e9-8f8c-4f4a-9dbf-06253e4562a8}    FilterWorkerItem
{8336e323-2e6a-4a04-937c-548f681839b3}    X509 Certificate Template AD Writable
{8352E327-B2EC-3331-9998-817EC5CC93B8}
{836FA1B6-1190-4005-B434-7ED921BE2026}    UserDictionary Class
{8398EE59-134A-420A-934A-D86A7F900D9A}    IsdbString Class
{83bb272f-7d5e-4b6e-9250-889893f0dac7}    Folder options command
{83bbcbf3-b28a-4919-a5aa-73027445d672}
{83BC5EC0-6F2A-11d0-A1C4-00AA00C16E65}
{842D84C9-C347-11D1-8F64-00C04FB611C7}    Interface Proxy Stub
{84a3a6bf-f1d8-496e-9f05-d3de70973152}    WWan Helper Class
{84D586C4-A423-11D2-B943-00C04F79D22F}    CustRg Class
{84e04a55-2d42-4909-86e3-62fd11483e8b}    Temporary Setup Files Cleanup
{84FC747A-1940-3D85-8819-EA53FC73DB1B}
{85074451-173D-4091-8648-C0E196BB363E}    WSUS App Publisher
{8509bb76-ffa3-4827-ba5e-2e786010f42f}    Item Set Operations Object
{850D1D11-70F3-4BE5-9A11-77AA6B2BB201}    CommonDialog Class
{85131630-480C-11D2-B1F9-00C04F86C324}    JS File Host Encode Object
{85131631-480C-11D2-B1F9-00C04F86C324}    VBS File Host Encode Object
{854CB94F-2279-4F7F-AC62-31E22E4D8899}    InfraConnectTask
{8570b44e-d109-42d3-be32-0f8d446669c5}    Close window command invocation
{85862EDA-F507-4d5b-ACA9-BB2C34A85682}    Microsoft XPS Rich Preview Handler
{8596E5F0-0DA5-11D0-BD21-00A0C911CE86}    File Writer
{85BBD920-42A0-1069-A2E4-08002B30309D}    Briefcase
{85cfccaf-2d14-42b6-80b6-f40f65d016e7}    Shortcut
{85e94d25-0712-47ed-8cde-b0971177c6a1}    Microsoft DocProp Rating Control
{85EB7D1F-7431-3E1E-A26E-EB1D16CB4ABB}
{860D36EE-748E-4B73-AE45-C33187E6F166}    MS IME 10 Character Applet
{86151827-E47B-45ee-8421-D10E6E690979}    Closed Captions Analysis Feature Segment
{863aa9fd-42df-457b-8e4d-0de1b8015c60}    Remote Printers
{863FA3AC-9D97-4560-9587-7FA58727608B}    SvcVwr 1.0 Object
{86422020-42A0-1069-A2E5-08002B30309D}    Network Context Menu Extension
{864A1288-354C-4D19-9D68-C2742BB14997}    User Event Timer
{865e5e76-ad83-4dca-a109-50dc2113ce9a}    Programs Folder and Fast Items
{8664DA16-DDA2-42AC-926A-C18F9127C302}    PSFactoryBuffer
{8670C736-F614-427b-8ADA-BBADC587194B}    DirectShow Plugin Manager
{86747AC0-42A0-1069-A2E6-08002B30309D}    Briefcase Folder
{868A2E25-D6C1-450b-8510-734A4AFEE8BC}    WlanConn LUA
{86bec222-30f2-47e0-9f25-60d11cd75c28}    Application Document Lists
```

Page 77

SOFTWARE OUTPUT.txt

```
{86c14003-4d6b-4ef3-a7b4-0506663b2e68}  Application Destination List
{86C86720-42A0-1069-A2E8-08002B30309D}  .exe drop target
{86d5eb8a-859f-4c7b-a76b-2bd819b7a850}  Virtual Factory for Usercpl
{86F80216-5DD6-4F43-953B-35EF40A35AEE}  CElevateWlanUi
{875CB1A1-0F29-45de-A1AE-CFB4950D0B78}  Audio Media Properties Handler
{87630419-6216-4ff8-a1f0-143562d16d5c}  Mobile Broadband Profile Settings Editor
{8770D941-A63A-4671-A375-2855A18EBA73}  InkRecognizerGuide Class
{877A0BB7-A313-4491-87B5-2E6D0594F520}
{877ca5ac-cb41-4842-9c69-9136e42d47e2}  File Backup Index
{877E4351-6FEA-11D0-B863-00AA00A216A1}  Plug In Distributor: IKsClock
{879fb53b-cba3-4fc8-b233-d9a93afa7fbc}  HomeGroup Task
{87BB326B-E4A0-4de1-94F0-B9F41D0C6059}  ThirdPartyEapDispatcherPeerRuntime
{87D66A43-7B11-4A28-9811-C86EE395ACF7}  Indexing Options Control Panel
{87DB1ADA-AA39-11D1-829F-00A0C906B239}
{87FC0268-9A55-4360-95AA-004A1D9DE26C}  DirectSoundWavesReverbDMO
{880ac964-2e34-4425-8cf2-86ada2c3a019}  State of play command
{8821c0e8-73ba-4448-8b46-23824e0d7831}  Location Association List
{883373C3-BF89-11D1-BE35-080036B11A03}  Summary Properties Page
{883FF1FC-09E1-48e5-8E54-E2469ACB0CFD}  SrControl Class
{8841d728-1a76-4682-bb6f-a9ea53b4b3ba}  LogonPasswordReset
{884e2000-217d-11da-b2a4-000e7bbb2b09}  ObjectId
{884e2001-217d-11da-b2a4-000e7bbb2b09}  ObjectId Collection
{884e2002-217d-11da-b2a4-000e7bbb2b09}  Binary Converter
{884e2003-217d-11da-b2a4-000e7bbb2b09}  X500 Distinguished Name
{884e2007-217d-11da-b2a4-000e7bbb2b09}  Csp Information
{884e2008-217d-11da-b2a4-000e7bbb2b09}  Csp Information Collection
{884e2009-217d-11da-b2a4-000e7bbb2b09}  Csp Status
{884e200b-217d-11da-b2a4-000e7bbb2b09}  X509 Public Key
{884e200c-217d-11da-b2a4-000e7bbb2b09}  X509 Private Key
{884e200d-217d-11da-b2a4-000e7bbb2b09}  X509 Extension
{884e200e-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Collection
{884e200f-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Key Usage
{884e2010-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Enhanced Key Usage
{884e2011-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Template Name
{884e2012-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Template
{884e2013-217d-11da-b2a4-000e7bbb2b09}  Alternative Name
{884e2014-217d-11da-b2a4-000e7bbb2b09}  Alternative Name Collection
{884e2015-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Alternative Names
{884e2016-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Basic Constraints
{884e2017-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Subject Key Identifier
{884e2018-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Authority Key Identifier
{884e2019-217d-11da-b2a4-000e7bbb2b09}  Smime Capability
{884e201a-217d-11da-b2a4-000e7bbb2b09}  Smime Capabilities Collection
{884e201b-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Smime Capabilities
{884e201c-217d-11da-b2a4-000e7bbb2b09}  Policy Qualifier
{884e201d-217d-11da-b2a4-000e7bbb2b09}  Policy Qualifier Collection
{884e201e-217d-11da-b2a4-000e7bbb2b09}  Certificate Policy
{884e201f-217d-11da-b2a4-000e7bbb2b09}  Certificate Policies Collection
{884e2020-217d-11da-b2a4-000e7bbb2b09}  X509 Extension Certificate Policies
{884e2021-217d-11da-b2a4-000e7bbb2b09}  X509 Extension MS Application Policies
{884e2022-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute
{884e2023-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Collection
{884e2024-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Extensions
{884e2025-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute ClientId
{884e2026-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Renewal Certificate
{884e2027-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Archivekey
{884e2028-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Archivekeyhash
{884e202a-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute OS Version
{884e202b-217d-11da-b2a4-000e7bbb2b09}  X509 Attribute Csp Provider
{884e202c-217d-11da-b2a4-000e7bbb2b09}  Cryptographic Attribute
{884e202d-217d-11da-b2a4-000e7bbb2b09}  Cryptographic Attribute Collection
{884e202e-217d-11da-b2a4-000e7bbb2b09}  Certificate Property
{884e202f-217d-11da-b2a4-000e7bbb2b09}  Certificate Properties Collection
```

Page 78

SOFTWARE OUTPUT.txt

```
{884e2030-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Friendly Name
{884e2031-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Description
{884e2032-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Auto-Enroll
{884e2033-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Request Originator
{884e2034-217d-11da-b2a4-000e7bbb2b09}  Certificate Property SHA-1 Hash
{884e2036-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Key Provider
Information
{884e2037-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Archived
{884e2038-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Backed-Up
{884e2039-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Enrollment
{884e203a-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Renewal
{884e203b-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Archived Key Hash
{884e203d-217d-11da-b2a4-000e7bbb2b09}  Signer Certificate
{884e203f-217d-11da-b2a4-000e7bbb2b09}  Name Value Pair
{884e2042-217d-11da-b2a4-000e7bbb2b09}  X509 CertificateRequest Pkcs10
{884e2043-217d-11da-b2a4-000e7bbb2b09}  X509 CertificateRequest Certificate
{884e2044-217d-11da-b2a4-000e7bbb2b09}  X509 CertificateRequest Pkcs7
{884e2045-217d-11da-b2a4-000e7bbb2b09}  X509 CertificateRequest Cmc
{884e2046-217d-11da-b2a4-000e7bbb2b09}  X509 Enrollment
{884e2049-217d-11da-b2a4-000e7bbb2b09}  X509 Enrollment WebClassFactory
{884e204c-217d-11da-b2a4-000e7bbb2b09}  Certificate Property Enrollment Policy
Server
{884e2050-217d-11da-b2a4-000e7bbb2b09}  X509 Enrollment Helper
{884e2051-217d-11da-b2a4-000e7bbb2b09}  X509 Machine Enrollment Factory
{8854F6A0-4683-4AE7-9191-752FE64612C3}  InkDivider Class
{8872FF1B-98FA-4D7A-8D93-C9F1055F85BB}  ATSC Tune Request Location Information
{88d96a05-f192-11d4-a65f-0040963251e5}  XML DOM Document 6.0
{88d96a06-f192-11d4-a65f-0040963251e5}  Free Threaded XML DOM Document 6.0
{88d96a07-f192-11d4-a65f-0040963251e5}  XML Schema Cache 6.0
{88d96a08-f192-11d4-a65f-0040963251e5}  XSL Template 6.0
{88d96a0a-f192-11d4-a65f-0040963251e5}  XML HTTP 6.0
{88d96a0b-f192-11d4-a65f-0040963251e5}  Server XML HTTP 6.0
{88d96a0c-f192-11d4-a65f-0040963251e5}  SAX XML Reader 6.0
{88d96a0e-f192-11d4-a65f-0040963251e5}  SAXAttributes 6.0
{88d96a0f-f192-11d4-a65f-0040963251e5}  MXXMLWriter 6.0
{88d96a10-f192-11d4-a65f-0040963251e5}  MXHTMLWriter 6.0
{88d96a11-f192-11d4-a65f-0040963251e5}  MXNamespaceManager 6.0
{896664F7-12E1-490f-8782-C0835AFD98FC}  Libraries delegate folder that appears in
Users Files Folder
{89BCB7A4-6119-101A-BCB7-00DD010655AF}
{89BCB7A5-6119-101A-BCB7-00DD010655AF}
{89BCB7A6-6119-101A-BCB7-00DD010655AF}
{89C2E132-C29B-11DB-96FA-005056C00008}  PBDA PTFilter
{89D83576-6BD1-4c86-9454-BEB04E94C819}  @%systemroot%\system32\mssvp.dll,-110
{89F9F7B0-8DE3-4AE0-8B41-109ABAB32151}  Microsoft WBEM Message Multi SendReceive
{8A01C400-A3E0-4F8D-A933-FF780F22BD87}  SnapinComponentData Class
{8A03E749-672E-446E-BF1F-2C11D233B6FF}
{8A22069C-1EF7-45D2-A409-219540D00A76}  Infrastructure Connect Page Class
{8A23E65E-31C2-11d0-891C-00A024AB2DBB}
{8A3E2E1E-A40B-4650-9FB4-30072A68E661}  ParseTracer Class
{8A667154-F9CB-11D2-AD8A-0060B0575ABC}  Microsoft DirectSound Wave
{8A674B49-1F63-11D3-B64C-00C04F79498E}  Utility Object for creating a Property Bag
backed by the Registry
{8A674B4C-1F63-11D3-B64C-00C04F79498E}  BDA Tuning Model Analog Radio Tuning Space
{8A674B4D-1F63-11D3-B64C-00C04F79498E}  BDA Tuning Model Analog TV Tuning Space
{8A6842BB-84DB-4EFA-99B9-06C850DF53FC}  WMPlayer NetworkPropPage Class
{8A734961-C4AA-4741-AC1E-791ACEBF5B39}
{8ac3587a-4ae7-42d8-99e0-0a6013eef90f}  Device Proxy MFT
{8ADD018C-5C5F-43C5-BE1E-07BAE85593B7}  HomeGroup Alpha Hosted Listener
{8ADE5386-8E9B-4F4C-ACF2-F0008706B238}
{8B7FBFE0-5CD7-494a-AF8C-283A65707506}  Default Location Class
{8BC3F05E-D86B-11D0-A075-00C04FB68820}  Windows Management and Instrumentation
{8be9f5ea-e746-4e47-ad57-3fb191ca1eed}  Listview Popup
```

Page 79

```
                         SOFTWARE OUTPUT.txt
    {8BEBCE8B-1AF0-4323-8B4D-36994567CAE1} Microsoft WMI Provider Subsystem InProc
Factory
    {8bf9a910-a8ff-457f-999f-a5ca10b4a885} Smartcard Credential Provider
    {8c1645b0-9864-465e-be75-990b030e4b11} XWizard Factory Generated Class (HomeGroup
Join Hook Page)
    {8C334A55-DDB9-491c-817E-35A6B85D2ECB} .
    {8C482DCE-2644-4419-AEFF-189219F916B9} HostPeerApis
    {8c4fb173-81ae-4399-9208-591a574a893f} Mobile Broadband CFE Page Class
    {8c4fce56-fc9a-4fcb-bd35-2ccabfd93844} Authentication UI Logon Settings
    {8C7461EF-2B13-11d2-BE35-3078302C2030} DEPRECATED: Component Categories cache
daemon
    {8c7eaf13-fbd6-4ed8-ac79-fb12fcd71326} SdEngine2 Class
    {8C89071F-452E-4E95-9682-9D1024627172}
    {8C9E8E1C-90F0-11D1-BA0F-00A0C906B239}
    {8CBEED49-18A6-4D9C-8EF5-E4DD9AB04A83} Windows Media Player
WMEncSourcePluginCommunicator Class
    {8CF89BCB-394C-49b2-AE28-A59DD4ED7F68} PSFactoryBuffer
    {8D04238E-9FD1-41C6-8DE3-9E1EE309E935} MSVidCtl DVD to Audio Renderer Composition
Segment
    {8D1C559D-84F0-4BB3-A7D5-56A7435A9BA6} Microsoft WBEM WMI Object Factory
    {8d1e5d4b-a99c-4408-b0f0-ccab9e5835a1} SuggestFilterWorker
    {8D26D9AA-5DA8-4b95-949A-B74954A229A6} Virtual Factory for Action Center CPL
    {8D4B04E1-1331-11d0-81B8-00C04FD85AB4} CLSID_ImnAccountManager
    {8d80504a-0826-40c5-97e1-ebc68f953792} OLE DocFile Property Handler
    {8D8B8E30-C451-421B-8553-D2976AFA648C} Sync Center Schedule Wizard
    {8DA6DB1C-8114-40c6-9D97-D2E7E9757D67} PSFactoryBuffer
    {8DB2180F-BD29-11D1-8B7E-00C04FD7A924} COMComponentRegistrar Class
    {8DE9C74C-605A-4acd-BEE3-2B222AA2D23D} NegationCondition Class
    {8e35b548-f174-4c7d-81e2-8ed33126f6fd} Biometrics navigate target object
    {8E528C21-9D52-4030-BA92-3481227ADDD1} WMPlayer PrivacyPropPage Class
    {8e827c11-33e7-4bc1-b242-8cd9a1c2b304} Merged Folder Categorizer
    {8e85d0ce-deaf-4ea1-9410-fd1a2105ceb5} Microsoft DocProp Inplace Multi-Value
Property Control
    {8e87e7b8-896b-4e67-bfa2-45c67d60ac3a} CPL Search Target Services
    {8E8F1601-AE98-3DAC-B48B-EC27C95A481E}
    {8E974B5A-A286-37DA-94F8-5872C500EB0E}
    {8EE97210-FD1F-4b19-91DA-67914005F020} Microsoft DocProp Inplace ML Edit Box
Control
    {8F0C5675-AEEF-11d0-84F0-00C04FD43F8F} AthWafer
    {8F914656-9D0A-4EB2-9019-0BF96D8A9EE6}
    {8FADC6A8-183E-4DFC-944A-84A323334B98} CFindNetPrinters Class
    {90087284-d6d6-11d0-8353-00a0c90640bf} Device Manager extension
    {900be39d-6be8-461a-bc4d-b0fa71f5ecb1} DiagnosticInfrastructureCustomHandler
    {900c0763-5cad-4a34-bc1f-40cd513679d5} User Account Control Check Service
    {905667aa-acd6-11d2-8080-00805f6596d2}
    {905b55a8-77f0-4d28-80dd-e46b1412343f} Execute OpenSearch view site command
    {90AA3A4E-1CBA-4233-B8BB-535773D48449} Taskband Pin
    {90b9bce2-b6db-4fd3-8451-35917ea1081b} CLSID_SearchMSExecute
    {90BE9587-37b7-477C-81A7-BA7C5C40FF81} MSASR Locale Handler Class (2057)
    {90F18417-F0F1-484E-9D3C-59DCEEE5DBD8} CIeAxiInstallerService Class
    {90f8c90b-04e0-4e92-a186-e6e9c125d664} Property Labels
    {913a6daa-57ee-4551-9ada-64d329d306a5} App Locations Icon Extract Extension
    {914feed8-267a-4baa-b8aa-21e233792679} Microsoft Preview Creator
    {91778246-9BE4-4713-A651-E833B853CC30}
    {91888BF6-FED1-4acd-9CB1-6C2F80AE58A3}
    {9193A8F9-0CBA-400E-AA97-EB4709164576} MSVidCtl SBE Source to Closed Caption
Composition Segment
    {91f39027-217f-11da-b2a4-000e7bbb2b09} X509 Enrollment Policy Active Directory
    {91f39028-217f-11da-b2a4-000e7bbb2b09} X509 Enrollment Policy Web Service
    {91f39029-217f-11da-b2a4-000e7bbb2b09} X.509 Policy Server List Manager Class
    {91f3902a-217f-11da-b2a4-000e7bbb2b09} X.509 Policy Server URL Class
    {9200689A-F979-4eea-8830-0E1D6B74821F} Virtual Factory for Recovery
    {92038079-b9ef-428f-87f0-0463fcb1272a} CLSID_VisibleIn
                              Page 80
```

SOFTWARE OUTPUT.txt
```
{9207d8c7-e7c8-412e-87f8-2e61171bd291}   Autoplay Known Devices Info
{92187326-72B4-11d0-A1AC-0000F8026977}   Game Controllers CPL Shell Extension
Default Property Sheets
{92337A8C-E11D-11D0-BE48-00C04FC30DF6}   prturl Class
{92396AD0-68F5-11d0-A57E-00A0C9138C66}   RowsetHelper
{923BFC9D-0F16-4B02-AF1B-39A2504D9873}   Additional Information Page Class
{92498132-4D1A-4297-9B78-9E2E4BA99C07}   NSSManager Class
{924ccc1b-6562-4c85-8657-d177925222b6}   Desktop Gadget Helper API
{9264B7DC-A82F-4AFD-89C8-4F399DA7B028}   VAN Settings Page Class
{926f41f7-003e-4382-9e84-9e953be10562}   ADTS Byte Stream Handler
{9271B890-7BBF-48DB-ACB3-F973DC34156D}   PSFactoryBuffer
{927971f5-0939-11d1-8be1-00c04fd8d503}   ADs Large Integer Object
{92A5010F-4404-4035-8D53-B87F5A736809}
{92ab5af7-a374-417e-b2e2-9b317353a322}   Microsoft Library Boolean Check Mark
Control
{92ad68ab-17e0-11d1-b230-00c04fb9473f}   STClient Class
{92b66080-5e2d-449e-90c4-c41f268e5514}   G711 ACM Wrapper MFT
{92B94828-1AF7-4e6e-9EBF-770657F77AF5}   Custom Composition Segment from iTV to
Stream Buffer Source
{92c85649-0892-4bc7-9b63-949f64149a26}   CMigrationPlugin Object
{92CC85F4-ACA4-4D72-94C8-49D1CAD0985F}   Infrastructure Connected Page Class
{92D2CC58-4386-45a3-B98C-7E0CE64A4117}   PSFactoryBuffer
{92dbad9f-5025-49b0-9078-2d78f935e341}   CLSID_PreviewMime
{92ED88BF-879E-448f-B6B6-A385BCEB846D}   MS Video Control Closed Captioning SI
Feature Segment
{9301E380-1F22-11D3-8226-D2FA76255D47}   DirectMusicContainer
{93126582-5402-4DB1-A102-33D330BC9B69}   Windows Media Player
WMEnc5Point1WavSourcePropertyPage Class
{9324DA94-50EC-4A14-A770-E90CA03E7C8F}   Windows Theme Manager 2 API
{9343812e-1c37-4a49-a12e-4b2d810d956b}   CLSID_SearchHome
{934a7048-1e4a-4d6e-9a9a-cb739f519b07}   XWizard Factory Generated Class (HomeGroup
Change Sharing Hook Page)
{934D4698-6A59-48f8-9F29-9FB30670320E}   Structured Query Helper Class
{93714ED0-53F0-11D2-9EE6-006008039E37}   Frame Rate Converter
{937C1A34-151D-4610-9CA6-A8CC9BDB5D83}   InkObject Class
{9381AF33-66A3-4D5A-8AF2-9515B1DC19A5}   PSFactoryBuffer
{93A094D7-51E8-485b-904A-8D6B97DC6B39}   SBE2 File Reader
{93a56381-e0cd-485a-b60e-67819e12f81b}   CLSID_CommonExplorerHost
{93AF0C51-2275-45D2-A35B-F2BA21CAED00}
{94297043-BD82-4DFD-B0DE-8177739C6D20}   DMO Wrapper Filter
{942B7909-A28E-49a1-A207-34EBCBCB4B3B}   MSVidCtl Analog Capture to CCA Composition
Segment
{942bc614-676c-464e-b384-d3202aaa02da}   INI Property Set Storage Handler
{94357B53-CA29-4b78-83AE-E8FE7409134F}   Drive Size Categorizer
{94426DE2-3211-11d2-A0DB-00C04F8EDCEE}
{944D4C00-DD52-11CE-BF0E-00AA0055595A}   DirectDraw Property Page
{9456A480-E88B-43EA-9E73-0B2D9B71B1CA}
{94596c7e-3744-41ce-893e-bbf09122f76a}   Smartcard Pin Provider
{948B45F7-EFB8-46fb-8704-B340D847227A}   Location Description Property Handler
{94AB5C27-C954-4218-B0A1-29640412EFBE}
{94abaf2a-892a-11d1-bbc4-00a0c90640bf}   About Device Manager
{94E03510-31B9-47a0-A44E-E932AC86BB17}   Windows Media Player Device Autoplay
{956FADED-2450-4ABB-9F8C-4629FAFEBB92}   HomeGroup Encryption
{95876EB0-90F0-11D1-BA0F-00A0C906B239}
{958A1709-3B44-11D1-AD74-00C04FC2ADC0}   RM Enlistment Helper
{958C59A0-3670-4FE0-B893-6998BB494402}   Microsoft WBEM Smart Object Marshaler
{95A18FCB-6850-420F-979B-CB3A149F2CC8}   EnumSTSALTINFO Class
{95CE8412-7027-11D1-B879-006008059382}   Shell Tree Walker
{961C1130-89AD-11CF-88A1-00AA004B9986}
{96236A71-9DBC-11DA-9E3F-0011114AE311}   PSFactoryBuffer
{96236A85-9DBC-11DA-9E3F-0011114AE311}   RdcLibrary Class
{96236A8F-9DBC-11DA-9E3F-0011114AE311}   SimilarityTraitsTable Class
{96236A90-9DBC-11DA-9E3F-0011114AE311}   SimilarityFileIdTable Class
```
Page 81

SOFTWARE OUTPUT.txt

```
{96236A91-9DBC-11DA-9E3F-0011114AE311}  Similarity Class
{967696C6-354C-4B5C-9CC8-BD9E1C480C77}  PimcSurrogate Class
{9694E38A-E081-46ac-99A0-8743C909ACB6}  html persistent handler for mapi email
{96AE8D84-A250-4520-95A5-A47A7E3C548B}  Parental Controls
{96BEC059-2052-4e44-8E11-123ACDC936FE}  WMDM Sync Property Page
{96FAC3B9-0273-4c0d-84F0-3A207A5EB38B}  Network Map
{97103AE5-6248-4E04-97B5-36663159967C}  windows Media Player WMEncTunerPropPage
Class
{973A7390-2608-3943-9015-D798D1217C08}
{9743B50B-3190-4061-8DA3-BE13AA02181E}  Infrastructure Progress Page Class
{975ABEDC-F64B-436d-ABFF-44B932459856}  windows Media Player OCXAdvancedPropPage
Class
{97e467b4-98c6-4f19-9588-161b7773d6f6}  Office Document Property Handler
{97EFC6C3-695B-4637-A6E6-9A28895F410E}  PSFactoryBuffer
{98037168-078f-4e5a-b235-a41aa5fd3bf5}  WMPMDE MPEG2 SINK ACTIVATE
{98042251-8C2B-4FC4-93E2-B1DB331EF5B9}  WMPlayer AdvancedPropPage Class
{98230571-0087-4204-b020-3282538e57d3}  Color Converter DMO
{98455561-5136-4d28-AB08-4CEE40EA2781}  MF Video Presenter
{987BBF42-5500-46D6-BAF0-A825828BC4EF}  windows Media Player WMEncFileSource Class
{989D1DC0-B162-11D1-B6EC-D27DDCF9A923}  XML Script Engine
{98af66e4-aa41-4226-b80f-0b1a8f34eeb4}  Manifest mime handler
{98AFF3F0-5524-11D0-8812-00A0C903B83C}  CertRequest Class
{98de59a0-d175-11cd-a7bd-00006b827d94}  Microsoft Office Persistent Handler
{991DA7E5-953F-435B-BE5E-B92A05EDFC42}  MSVidCtl Stream Buffer Source To Generic
Sink Composition segment
{992CFFA0-F557-101A-88EC-00DD010CCC48}  Network Connections
{995C996E-D918-4a8c-A302-45719A6F4EA7}  Shell Hardware Mixed Content Handler
{996d2d72-4c19-47f8-8f58-0bb13e80a659}  HomeGroup Balloon
{99969a8f-27e6-4adf-ab9f-b5b5e90d4733}  Verb Handler for launching verbs on
properties of items
{99c0179c-c20c-488c-a510-bd779b9376ae}
{99cdfdaf-3573-4d97-bc06-d7c36627edef}  Mobile Broadband Connect Failure Page
Class
{99D54F63-1A69-41AE-AA4D-C976EB3F0713}  VMR Allocator Presenter
{99E89F48-A745-416d-A4E0-ECF53C65DFA0}  DynamicRenderer Class
{99EB9580-04EC-4B4C-99F5-52B616D444D9}  MSASR Locale Handler Class (1031)
{9a02e012-6303-4e1e-b9a1-630f802592c5}  Packed Property Storage Object
{9A5EA990-3034-4D6F-9128-01F3C61022BC}  GameExplorer Class
{9A653086-174F-11D2-B5F9-00104B703EFD}  Microsoft WBEM WBEM Class Object
{9a97f12a-6b73-4dc4-b3c1-e9244c03adac}  shell foreground window setter
{9AA0422B-E5C5-4A6B-ACEC-C96E2E05B353}  CIsdb Class
{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}  ShellItem Shell Namespace helper
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}  CAutoUpdate Class 1.0
{9B496CE1-811B-11CF-8C77-00AA006B6814}  IAMTimecodeReader
{9B55AA0E-1BC2-46e4-B306-DF9BDFDCC644}
{9B77C0F2-8735-46c5-B90F-5F0B303EF6AB}  CAsfTocParser
{9BA05971-F6A8-11CF-A442-00A0C90A8F39}  Microsoft Shell Folder view Router
{9BA05972-F6A8-11CF-A442-00A0C90A8F39}  ShellWindows
{9BCE6E2B-116B-420F-928B-5356D1629979}
{9BF8D948-5C56-450e-BAF8-D6144C6E81CB}  SqlGenerator Class
{9C1CC6E4-D7EB-4EEb-9091-15A7C8791ED9}  InkRenderer Class
{9C24A977-0951-451A-8006-0E49BD28CD5F}
{9C502F01-0D36-4f16-8AC9-8693E0D84E44}  WMPlayer CDBurnPropPage Class
{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF}  Sync Center Folder
{9CB535DD-4354-42a1-8281-BBB58DEFA741}  Performance Control Panel
{9CD31617-B303-4F96-8330-2EB173EA4DC6}
{9CD64701-BDF3-4D14-8E03-F12983D86664}  BDA Tuning Model DVB Terrestrial Locator
{9cfc2df3-6ba3-46ef-a836-e519e81f0ec4}  Property System Apartment Class Factory
{9D3C0751-A13F-46a6-B833-B46A43C30FE8}  MAPI Shell Context Menu
{9D71A98F-1E45-42EC-AF3D-FA13BEFB955C}  Manual Connect Page Class
{9D745ED8-C514-4D1D-BF42-751FED2D5AC7}  HNetCfg.FwProduct
{9DAC2C1E-7C5C-40eb-833B-323E85A1CE84}
{9DBD2C50-62AD-11d0-B806-00C04FD706EC}  Property Thumbnail Handler
```

Page 82

SOFTWARE OUTPUT.txt

```
{9DCC3CC8-8609-4863-BAD4-03601F4C65E8}   LatLongReportFactory Class
{9DD35758-AAF5-4894-ADAA-77A492F54E0A}   WlanDlgNonUIPage Class
{9DE85094-F71F-44f1-8471-15A2FA76FCF3}   InkWordList Class
{9DFFD99C-536B-4D0F-B70F-E875B78A3477}
{9E175B68-F52A-11D8-B9A5-505054503030}   Search Gathering Manager
{9E175B69-F52A-11D8-B9A5-505054503030}   Search Embedded Gathering Manager
{9E175B6C-F52A-11D8-B9A5-505054503030}   Search Gatherer Transaction
{9E175B6D-F52A-11D8-B9A5-505054503030}   Search Gatherer Notification
{9E175B6E-F52A-11D8-B9A5-505054503030}   Microsoft Embedded Search Gatherer
Notification
{9E175B70-F52A-11D8-B9A5-505054503030}   Search Gatherer Language Resource Pool
{9E175B74-F52A-11D8-B9A5-505054503030}   Search Gatherer Plug-in
{9E175B76-F52A-11D8-B9A5-505054503030}   Windows Search Service File Protocol
Handler
{9E175B7F-F52A-11D8-B9A5-505054503030}   Search Back off Controller
{9E175B8A-F52A-11D8-B9A5-505054503030}   Search command creator object
{9E175B8B-F52A-11D8-B9A5-505054503030}   Windows Search Data Source
{9E175B8D-F52A-11D8-B9A5-505054503030}   Search FilterRegistration Class
{9E175B8E-F52A-11D8-B9A5-505054503030}   Search LoadLangRes Class
{9E175B90-F52A-11D8-B9A5-505054503030}   Full Text SQL Parser
{9E175B98-F52A-11D8-B9A5-505054503030}   Search Neutral Word Breaker Resources
{9E175BA8-F52A-11D8-B9A5-505054503030}   Search Null Word Breaker
{9E175BA9-F52A-11D8-B9A5-505054503030}   Search Gatherer Log File Provider
{9E175BB7-F52A-11D8-B9A5-505054503030}   Windows Search Service Tripoli Indexer
Engine
{9E175BB8-F52A-11D8-B9A5-505054503030}   Windows Search Service Jet Property
Storage Engine
{9E358D23-02B2-4CCD-9FEE-6B75EE8DD5CA}   PSFactoryBuffer
{9E51E0D0-6E0F-11d2-9601-00C04FA31A86}
{9E56BE60-C50F-11CF-9A2C-00A0C90A90CE}   Mail Service
{9E56BE61-C50F-11CF-9A2C-00A0C90A90CE}   Desktop Shortcut
{9E704F44-90F0-11D1-BA0F-00A0C906B239}
{9E77AAC4-35E5-42A1-BDC2-8F3FF399847C}   Stream Buffer Sink Segment
{9E797ED0-5253-4243-A9B7-BD06C58F8EF3}   iTV Playback Feature Segment
{9EBB177D-0161-4e2c-81B0-E15D586CFC9F}   PSFactoryBuffer
{9EC4B4F9-3029-45ad-947B-344DE2A249E2}   Urlmon Scheme Handler
{9ecb380c-2333-4c68-9691-a569fe446820}   MAPISendMailServer
{9ecf51f8-cfb1-458d-9485-f5a231afd22f}   CLSID_XMLAutoList
{9ED4692C-90F0-11D1-BA0F-00A0C906B239}
{9ED96B20-73AA-11D2-952C-0060081840BC}   Frame Rate Converter Property Page
{9ED96B21-73AA-11D2-952C-0060081840BC}   Audio Repackager Property Page
{9ED96B22-73AA-11D2-952C-0060081840BC}   Dexter Queue
{9EFD4CF2-0BAA-350B-9D73-0974077B2F7B}
{9F007F18-9C24-4630-8B3E-61F96280C593}   Microsoft WBEM Rpc Message Receiver
{9F0139EC-2195-42d7-A7B6-41E1DA530AD9}   File data caching class
{9F36C194-166C-4cbf-B7EA-BF039F950172}   PeerGroup Wrapper
{9F377D7E-E551-44f8-9F94-9DB392B03B7B}   CProvideWinSATVisuals Class
{9F50E8B1-9530-4DDC-825E-1AF81D47AED6}   MSVidCtl Analog TV to StreamBufferSource
Composition Segment
{9F66347C-60C4-4C4D-AB58-D2358685F607}   SettingsEngine Class
{9F7D7BB5-20B3-11DA-81A5-0030F1642E3C}   InkRecognizers Class
{9FD4E808-F6E6-4e65-98D3-AA39054C1255}   System Recovery
{9FE63AFD-59CF-4419-9775-ABCC3849F861}   Mobile Broadband Puk1 Page Class
{9ff7242c-364d-425d-95ce-c64f8ee140d1}   CLSID_FindExecute
{a015411a-f97d-4ef3-8425-8a38d022aebc}   CameraControl2 Class
{A0227FFC-3AA7-4dc3-9FD7-125745C9EAF6}   Infrared
{A0275511-0E86-4ECA-97C2-ECD8F1221D08}
{A02797fc-C4AE-418C-AF95-E637C7EAD2A1}
{A03CD5F0-3045-11CF-8C44-00AA006B6814}   IAMExtTransport
{a07034fd-6caa-4954-ac3f-97a27216f98a}   Query file associations
{A08AF898-C2A3-11d1-BE23-00C04FA31009}   Windows Mail Envelope
{A09C534C-0057-462E-8402-2A21D38BFCA1}   New Network category Task
{A09CCA86-27BA-4F39-9053-121FA4DC08FC}
```

Page 83

```
                           SOFTWARE OUTPUT.txt
    {A0A7A57B-59B2-4919-A694-ADD0A526C373}  Tearless Window Presenter
    {A0B9B497-AFBC-45AD-A8A6-9B077C40D4F2}  Custom Composition Segment from Encoder to
Time Shift Sink
    {a0d018ee-1100-4389-ab44-464faf001288}  Authentication UI Logon Sound
    {A0F93E27-F05D-4153-A151-F3720369A4C7}  Microsoft WMI Signed Driver Provider
    {A1006DE3-2173-11d2-9A7C-00C04FA309D4}  CLSID_COE5Import
    {a11850eb-4501-4dea-9ef5-1d37f57d247d}  Mobile Broadband Create Profile Page Class
    {A11DB3DC-5FF6-4a0b-AEE6-29BCAC1E11E0}
    {a1570149-e645-4f43-8b0d-409b061db2fc}  EnumBthMtpConnectors Class
    {A1607060-5D4C-467a-B711-2B59A6F25957}  AltTab
    {A167B942-CD17-4d00-BDD9-8FDC2DC158F2}
    {a16e1bff-a80d-48ad-aecd-a35c005685fe}  IMA ADPCM ACM Wrapper MFT
    {A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980}  Collection of BDA Tuning Model Component
Types(Broadcast Substream Types)
    {A1F4E726-8CF1-11D1-BF92-0060081ED811}  WIA Device Manager
    {A25821B5-F310-41BD-806F-5864CC441B78}  WlanPref LUA
    {a2a9545d-a0c2-42b4-9708-a0b2badd77c8}  Start Menu Pin
    {A2D75874-6750-4931-94C1-C99D3BC9D0C7}  Microsoft Windows Defender
    {A2D8CFE7-7BA4-4bad-B86B-851376B59134}  Windows Parental Controls
    {A2E3074E-6C3D-11D3-B653-00C04F79498E}  BDA Tuner Device Segment
    {A2E3074F-6C3D-11D3-B653-00C04F79498E}
    {A2E30750-6C3D-11D3-B653-00C04F79498E}  BDA Tuning Model ATSC Tuning Space
    {A2E6DDA0-06EF-4df3-B7BD-5AA224BB06E8}  ImageFile Class
    {A32552C5-BA61-457A-B59A-A2561E125E33}  UPnPDevice Class
    {A373F500-7A87-11D3-B1C1-00C04F68155C}  Windows Search Service Client Side Cache
Protocol Handler
    {a3b3c46c-05d8-429b-bf66-87068b4ce563}  Action Center Notification Manager
    {A3C97737-76D9-4f5f-B917-4DE47FE023C8}  CWinsatWMI Class
    {A3E41207-BE04-492A-AFF0-19E880FF7545}  WMI instrumentation:
Win32_ComputerShutdownEvent
    {A3ECBC41-581A-4476-B693-A63340462D8B}  Filter Graph Private Thread
    {a42c2ccb-67d3-46fa-abe6-7d2f3488c7a3}  Windows RTF Previewer
    {A45AEC2B-549E-405F-AF3E-C6B03C4FDFBF}  ToggleDMRAuthorization
    {A470F8CF-A1E8-4f65-8335-227475AA5C46}  Encryption Context Menu
    {a47401f6-a8a6-40ea-9c29-b8f6026c98b8}
    {A47979D2-C419-11D9-A5B4-001185AD2B89}  Network List Manager
    {A4A1A128-768F-41E0-BF75-E4FDDD701CBA}  PSFactoryBuffer
    {A4B544A1-438D-4B41-9325-869523E2D6C7}  TF_CategoryMgr
    {a4c31131-ff70-4984-afd6-0609ced53ad6}  Shell ChkdskEx Dialog
    {A5270F6C-19EC-4E17-9EA1-A7074276B9B9}  Windows Search Items Changed Sink
    {a542e116-8088-4146-a352-b0d06e7f6af6}  Address EditBox
    {A55803CC-4D53-404c-8557-FD63DBA95D24}  WPDShextAutoplay
    {a5a3563a-5755-4a6f-854e-afa3230b199f}  Library Folder
    {A5B020FD-E04B-4e67-B65A-E7DEED25B2CF}  TabletManager Class
    {A5EFE073-B16F-474f-9F3E-9F8B497A3E08}  PSFactoryBuffer
    {A6098E79-9C50-4F87-8973-5FB4532C93D8}  BTConnectionUi Class
    {A6207B2E-7CDD-426A-951E-5E1CBC5AFEAD}  PSFactoryBuffer
    {a671c915-d95d-4135-b2c3-089356ca694f}  Nla Helper Class
    {a677570a-2ba2-4e9a-b2e2-8a02cd8b4fd3}  CoPrintIsolationHost Class
    {a6914418-134b-4bb8-8e3d-7fef7f456caf}  CRasDiagHelper Object
    {A6A3E580-083F-471b-8F08-87D34F678C95}  RDB AutoPlay Handler Class
    {A6EE35C6-87EC-47DF-9F22-1D5AAD840C82}
    {A6F1684D-AED6-401b-9786-A3E3B53C6641}  Parental Controls Control Panel
    {a76de978-f3eb-4a4f-9f99-304ad619e2ab}  State of OpenSearch view site command
    {A7A63E5C-3877-4840-8727-C1EA9D7A4D50}  Secure Startup
    {A8040703-2640-48B7-96CD-BC8108A4E8F1}  SnapinComponent Class
    {A82E50BA-8E92-41eb-9DF2-433F50EC2993}  MP3 Byte Stream Handler
    {A83EF168-CA8D-11D2-B33D-00104BCC4B4A}  CLSID_IntProv
    {a86ca2f1-af74-4a74-980b-e185d4ca01b0}  HomeGroup Task
    {A8792A31-F385-493C-A893-40F64EB45F6E}  PSFactoryBuffer
    {A879E3C4-AF77-44fb-8F37-EBD1487CF920}  PSFactoryBuffer
    {a8cc4a39-8f83-44eb-a73e-e2848c4f585f}  WMPMDE RTSP SINK ACTIVATE
    {A8DCF3D5-0780-4EF4-8A83-2CFFAACB8ACE}  BDA Tuning Model ATSC Component Type Class
                                   Page 84
```

SOFTWARE OUTPUT.txt

```
(Broadcast Substream Type)
 {A8DFB9A0-8A20-479F-B538-9387C5EEBA2B}   VMR Mixer 9
 {A8E64375-B645-4314-9EFC-C085981786FA}
 {A9397D66-3ED3-11D1-8D99-00C04FC2E0C7}
 {A9710FB5-1840-4224-BD42-86831E28E43A}   RemMdmObj Class
 {A9A33436-678B-4c9c-A211-7CC38785E79D}   WinSAT Task Manger Task
 {a9ae6c91-1d1b-11d2-b21a-00c04fa357fa}   LW Identities
 {A9B48EAC-3ED8-11d2-8216-00C04FB687DA}   Content Indexer Cleaner
 {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}   Search Gatherer Inline Notification
 {A9CF0EAE-901A-4739-A481-E35B73E47F6D}   Microsoft DocProp Inplace Edit Box Control
 {A9F738C8-6B96-41FA-A155-15ECD67275D0}   Windows Search Protocol Handler Search
Connector Creator
 {A9FC132B-096D-460B-B7D5-1DB0FAE0C062}   RMGetLicense Class
 {AA000926-FFBE-11CF-8800-00A0C903B83C}   CertServerPolicy Class
 {AA10385A-F5AA-4EFF-B3DF-71B701E25E18}   Wordpad ODT Document Filter
 {AA160628-8775-46e3-837C-F7A2AE66E2F5}   Quarantine SoH Protocol processor class
 {aa28fbc7-59f1-4c42-9fd8-ba2be27ea319}   Select All command invocation
 {AA558FA2-A340-4a23-B765-614BA827CE1D}   SppInstallerFactory Class
 {AA7E3C50-864C-4604-BC04-8B0B76E637F6}
 {AAA288BA-9A4C-45B0-95D7-94D524869DB5}   WPDShServiceObj Class
 {AABE54D4-6E88-4c46-A6B3-1DF790DD6E0D}   Themes tree item callback object for
sysdm.cpl
 {AABFB2FA-3E1E-4A8f-8977-5556FB94EA23}
 {AAC46A37-9229-4fc0-8CCE-4497569BF4D1}   InkRecognizerContext Class
 {ab0b37ec-56f6-4a0e-a8fd-7a8bf7c2da96}   CLSID_ExplorerHostCreator
 {AB2ECE69-56D9-4F28-B525-DE1B0EE44237}   PSFactoryBuffer
 {AB517586-73CF-489c-8D8C-5AE0EAD0613A}   Microsoft DocProp Custom Draw Percent Full
Control
 {AB93B6F1-BE76-4185-A488-A9001B105B94}   BDEUILauncher Class
 {AB944620-79C6-11D1-88F9-0080C7D771BF}   Event Publisher
 {AB9D6472-752F-43F6-B29E-61207BDA8E06}   RDP DShow Video Renderer
 {ABB27087-4CE0-4E58-A0CB-E24DF96814BE}   InertiaProcessor Class
 {ABBA0005-3075-11D6-88A4-00B0D0200F88}   ATSCTerrestrial Class
 {ABBA0006-3075-11D6-88A4-00B0D0200F88}   CDvb Class
 {ABBA001B-3075-11D6-88A4-00B0D0200F88}   DigitalCable Class
 {abd2ad24-f1ff-47ad-82de-3a1edf38e7a1}   HomeGroup Task
 {ABDBD0B1-7D54-49fb-AB5C-BFF4130004CD}   PSFactoryBuffer
 {ABE40035-27C3-4A2F-8153-6624471608AF}   MSVidCtl Digital TV to StreamBufferSource
Composition Segment
 {AC3AC249-E820-4343-A65B-377AC634DC09}   WinBio Credential Provider
 {AC75D454-9F37-48f8-B972-4E19BC856011}
 {AC82FF6D-E524-4c0f-8D0B-0C74C1ECAAEA}   InkCursors Class
 {ACD453BC-C58A-44D1-BBF5-BFB325BE2D78}   Microsoft MPEG-2 Audio Encoder
 {ACD857DF-E3D9-36DD-A0AD-7D155D326CE8}
 {AD1841CF-0EC5-4b59-ACC4-8329EED299F9}
 {AD4C1B00-4BF7-422F-9175-756693D9130D}   PSFactoryBuffer
 {AD581B00-7B64-4E59-A38D-D2C5BF51DDB3}   WindowsMediaLibrarySharingServices Class
 {AD6C8934-F31B-4F43-B5E4-0541C1452F6F}   WST Pager
 {ad763fa6-3b90-41ab-bd44-4f832beee55f}   Windows Media Network Source Plugin
 {AD8E510D-217F-409B-8076-29C5E73B98E8}   Stream Buffer Source
 {ad974ae2-e292-4083-a280-0342d68daf55}   Updatable Item Set
 {ADAB9B51-4CDD-4af0-892C-AB7FA7B3293F}   Group Policy Service User Profile
Notification
 {adacedf4-9c34-430e-a65f-488f0ab491da}
 {ADB880A4-D8FF-11CF-9377-00AA003B7A11}
 {ADB880A6-D8FF-11CF-9377-00AA003B7A11}   HHCtrl Object
 {ADB9F5A4-E73E-49b8-99B6-2FA317EF9DBC}   Windows ScreenSaver Properties
 {ADBE6DEC-9B04-4A3D-A09C-4BB38EF1351C}   XAML Browser Application
 {add36aa8-751a-4579-a266-d66f5202ccbb}   Print Ordering via the Web
 {ADE6444B-C91F-4E37-92A4-5BB430A33340}   AppEventsDHTMLConnector 1.0 Object
 {ADF95821-DED7-11D2-ACBE-0080C75E246E}   Property Setter
 {AE03A0A5-DE98-45ff-8016-DDEFF70BCF61}   SAL File
 {AE054212-3535-4430-83ED-D501AA6680E6}   Shell Name Space ListView
```

Page 85

```
                           SOFTWARE OUTPUT.txt
    {AE1E00AA-3FD5-403C-8A27-2BBDC30CD0E1}  Home Networking NAT Traversal via UPnP
Configuration Manager
    {ae2079d8-d764-4d79-ab4d-3543847a1a2c}
    {AE62C05D-0A02-30E7-9B51-E9D4DD157207}
    {AE8AFD54-5B57-4961-8A9B-12ADF23B696A}
    {AE9472BF-B0C3-11D2-8D24-00A0C9441E20}  GrfCache Class
    {AEB16279-B750-48f1-8586-97956060175A}  MF ASF Property Handler
    {AEC17CE3-A514-11D1-AFA6-00AA0024D8B6}  DirectMusicSynthSink
    {AEE3E4A8-EF01-4024-A0F1-809D9B096E14}  Windows Media Player Encoder Helper Class
    {AEF1693C-839C-4066-82D6-6CC0324C9D20}  Microsoft MPEG-2 Video Encoder Property
Page
    {AF02484C-A0A9-4669-9051-058AB12B9195}  File Save Dialog Legacy
    {AF2440F6-8AFC-47d0-9A7F-396A0ACFB43D}  PSFactoryBuffer
    {AF2AC6EE-2B16-4756-9475-F319E543EFAA}  SOAPRequest Class
    {AF4F6510-F982-11d0-8595-00AA004CD6D8}  Registry Tree Options Utility
    {AF604EFE-8897-11D1-B944-00A0C90312E1}  Microsoft Common Browser Architecture
    {AF95DC76-16B2-47F4-B3EA-3C31796693E7}
    {AF9F2C0D-6B9F-4e32-A94D-A3E235A31BF7}  XML property store
    {AFB40FFD-B609-40A3-9828-F88BBE11E4E3}  Server XML HTTP 3.0
    {AFB6C280-2C41-11D3-8A60-0000F81E0E4A}  MPEG-2 Demultiplexer
    {AFBA6B42-5692-48EA-8141-DC517DCF0EF1}  Server XML HTTP
    {AFD7F94B-1627-436c-80C8-B464AA21CAD3}  WMPlayer SecurityPropPage Class
    {b020b123-89b9-46c6-8509-a8bf70447fea}  PSFactoryBuffer
    {B0210780-89CD-11d0-AF08-00A0C925CD16}  DirectSoundCapture Object
    {B021FF57-A928-459c-9D6C-14DED0C9BED2}  PrinterQueueView Class
    {B0395DA5-6A15-4E44-9F36-9A9DC7A2F341}  MMC IconControl class
    {b040ea9e-3f5e-48c9-bcdc-304e9d02851f}  CSdGITManager Class
    {B056521A-9B10-425E-B616-1FCD828DB3B1}  PSFactoryBuffer
    {B084785C-DDE0-4d30-8CA8-05A373E185BE}  NSC Byte Stream Handler
    {B091E540-83E3-11CF-A713-0020AFD79762}  File Types Page
    {B0A2AB46-F612-4469-BEC4-7AB038BC476C}  WMI High Performance Cooker
    {B0A8F3CF-4333-4bab-8873-1CCB1CADA48B}  Drive Type Categorizer
    {b0c43320-2315-44a2-b70a-0943a140a8ee}  XPS Signature Manager
    {B0D17FC2-7BC4-11d1-BDFA-00C04FA31009}  CLSID_IFontCache
    {B0EDF163-910A-11D2-B632-00C04F79498E}  MS TV Video Control
    {B106900C-4E8D-4147-8B22-CC60C6B285A8}  Windows Media Player Compositing Mixer
    {B12AE898-D056-4378-A844-6D393FE37956}  Windows ThemeUI Pages
    {b1325ef5-dd4d-4988-a2b3-c776ad45d0d6}  Authentication UI Legacy Shutdown Dialog
    {b155bdf8-02f0-451e-9a26-ae317cfd7779}  delegate folder that appears in Computer
    {B196B286-BAB4-101A-B69C-00AA00341D07}  PSFactoryBuffer
    {B1EBFC28-C9BD-47A2-8D33-B948769777A7}
    {B210D694-C8DF-490d-9576-9E20CDBC20BD}  Color Calibration Loader
    {b27b520e-46db-4720-b9c5-5f80acab23a4}  HomeGroup Task
    {b2952b16-0e07-4e5a-b993-58c52cb94cae}  CLSID_DBFolder
    {B2A7FD52-301F-4348-B93A-638C6DE49229}  WMPSkinMngr Class
    {b2b4fb61-d2dd-4ddd-8001-20f98c6577ef}  Microsoft Query Edit Control
    {B2C761C6-29BC-4f19-9251-E6195265BAF1}  Color Management
    {B2E8D89A-7A99-4b43-9638-DF4FF83EAC11}
    {B2F2E083-84FE-4a7e-80C3-4B50D10D646E}  Default Category Provider
    {B2F3A67C-29DA-4C78-8831-091ED509A475}  Microsoft Network Provider
    {B2F586D4-5558-49D1-A07B-3249DBBB33C2}  DirectSoundBufferConfig Object
    {B323F8E0-2E68-11D0-90EA-00AA0060F86C}  StillImage
    {B32D3949-ED98-4DBB-B347-17A144969BBA}  Sync Center Item Properties Extension
    {B32F4002-BB27-45FF-AF4F-06631C1E8DAD}  PSFactoryBuffer
    {B33F0D7A-1571-4022-B710-D26E9B87DEB8}  Autoplay Content Handler
    {B35EA47E-FA71-34FD-B7E2-EBC050A4FB5A}
    {B3FD5602-EB0F-415E-9F32-75DA391D6BF9}  ExecutivePlatform
    {B3FF88A4-96EC-4CC1-983F-72BE0EBB368B}  Rsop Logging Mode Provider
    {B401C5EB-8457-427F-84EA-A4D2363364B0}  MSVidCtl FilePlayback to Video Renderer
Composition Segment
    {B4124623-FC0E-47CE-BCA9-126A6104ADA1}  JournalReader Class
    {B4B3AECB-DFD6-11d1-9DAA-00805F85CFE3}
    {B4C8DF59-D16F-4042-80B7-3557A254B7C5}  Bluetooth PAN Profile Class Manager
                                  Page 86
```

```
                          SOFTWARE  OUTPUT.txt
   {B4D85BBD-C1E6-4F2B-BF43-75CB28500A08}  Windows Media Player TunerHelper Class
   {B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}  Other Users Folder
   {B54E85D9-FE23-499F-8B88-6ACEA713752B}
   {B5607793-24AC-44c7-82E2-831726AA6CB7}  Free Space Categorizer
   {B5730A90-1A2C-11CF-8C23-00AA006B6814}  IAMExtDevice
   {b5827163-52b0-42c2-940f-f1d72cab1251}  WMPMDE NETCHANNEL ACTIVATE
   {b5866878-bd99-11d0-b04b-00c04fd91550}  TypeFactory
   {B5965ACC-842D-4ABE-A618-9292BB3EE666}  MSASR Locale Handler Class (2052)
   {b5a60a9e-a4c7-4a93-ac6e-0b76d1d87dc4}  Device Center Scan Context Menu Extension
   {B5C8B898-0074-459F-B700-860D4651EA14}
   {B5EBAFB9-253E-4A72-A744-0762D2685683}
   {b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}  MSAA AccPropServices
   {B64016F3-C9A2-4066-96F0-BD9563314726}  BDA Tuning Model DVB-Satellite Tuning
Space
   {B699E5E8-67FF-4177-88B0-3684A3388BFB}  UpdateSearcher Class
   {B6C292BC-7C88-41EE-8B54-8EC92617E599}  WIA Device Manager 2
   {B708457E-DB61-4C55-A92F-0D4B5E9B1224}  MMCViewExt 1.0 Object
   {b70cc729-28ae-11dd-9676-000000000000}  MBN Pin Unblock page
   {B72F8FD8-0FAB-4dd9-BDBF-245A6CE1485B}  QueryParser Class
   {b75ac000-9bdd-11d0-852c-00c04fd8d503}  ADs Access Control Entry Object
   {B76AD54C-51A2-4230-B516-2CCAA95F8D29}  Enable the Desktop Window Manager tree
item callback object for sysdm.cpl
   {b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}  ShellItemArray Shell Namespace helper
   {B77C4C36-0154-4c52-AB49-FAA03837E47F}  CLSID_PublicationServicesServer
   {B7BBD408-F09C-4aa8-B65E-A00B8FE0F0B9}  Windows Theme Preview API
   {B80AB0A0-7416-11D2-9EEB-006008039E37}  MJPEG Compressor
   {B8558612-DF5E-4F95-BB81-8E910B327FB2}  Sync Center (Private)
   {b85ea052-9bdd-11d0-852c-00c04fd8d503}  ADs Access Control List Object
   {B87BEB7B-8D29-423F-AE4D-6582C10175AC}  Video Mixing Renderer
   {B890AF56-AC8C-11D1-8CB7-00C04FC3261D}  CLBDTDispenser Class
   {b8967f85-58ae-4f46-9fb2-5d7904798f4b}  Property System
   {B9162A23-45F9-47CC-80F5-FE0FE9B9E1A2}  Bidi Spooler APIs
   {b91a4db4-3630-11dc-9eaa-00161718cf63}  Burn command invocation
   {B92E345D-F52D-41F3-B562-081BC772E3B9}
   {b958f73c-9bdd-11d0-852c-00c04fd8d503}  ADs Security Descriptor Object
   {B977CB2D-EC6E-4A8F-BFFE-D18682BB0D52}  IShareMediaSettingsWriter
   {b9815375-5d7f-4ce2-9245-c9d4da436930}  CLSID_PreviewEmail
   {B98A2BEA-7D42-4558-8BD1-832F41BAC6FD}  Backup And Restore
   {B9931692-A2B3-4FAB-BF33-9EC6F9FB96AC}  TF_LangBarItemMgr
   {b9b61a03-caa7-43bb-b859-acd26d73b3f7}  CLSID_ResultHandlerFactory
   {B9E84FFD-AD3C-40A4-B835-0882EBCBAAA8}  UPnPDevices Class
   {BA126AD1-2166-11D1-B1D0-00805FC1270E}  Network Connection Manager Class
   {BA126AD2-2166-11D1-B1D0-00805FC1270E}  Network Connection Manager Connection
Enumerator Class
   {BA126AD3-2166-11D1-B1D0-00805FC1270E}  LAN Connection Manager Class
   {BA126AD4-2166-11D1-B1D0-00805FC1270E}  LAN Connection Manager Connection
Enumerator Class
   {BA126AD5-2166-11D1-B1D0-00805FC1270E}  WAN Connection Manager Class
   {BA126AD6-2166-11D1-B1D0-00805FC1270E}  WAN Connection Manager Connection
Enumerator Class
   {BA126AD7-2166-11D1-B1D0-00805FC1270E}  Dial-up Connection Class
   {BA126AD8-2166-11D1-B1D0-00805FC1270E}  Network Group Policies for NLA Class
   {BA126AD9-2166-11D1-B1D0-00805FC1270E}  Inbound Connection Class
   {BA126ADB-2166-11D1-B1D0-00805FC1270E}  LAN Connection Class
   {BA126ADD-2166-11D1-B1D0-00805FC1270E}  Inbound Connection Manager Class
   {BA126ADE-2166-11D1-B1D0-00805FC1270E}  Inbound Connection Manager Connection
Enumerator Class
   {BA126ADF-2166-11D1-B1D0-00805FC1270E}  Network Install Queue
   {BA126AE0-2166-11D1-B1D0-00805FC1270E}  Shared Access Connection Manager
   {BA126AE1-2166-11D1-B1D0-00805FC1270E}  Shared Access Connection Manager
Enumerated Connection
   {BA126AE2-2166-11D1-B1D0-00805FC1270E}  Shared Access Connection
   {BA126AE3-2166-11D1-B1D0-00805FC1270E}  Home Networking Connections Ultility Class
                              Page 87
```

SOFTWARE OUTPUT.txt

```
{BA126AE5-2166-11D1-B1D0-00805FC1270E}    Network Connection Manager Class 2
{BA126E01-2166-11D1-B1D0-00805FC1270E}    Connection Manager LUA Inproc Object
{BA126F01-2166-11D1-B1D0-00805FC1270E}    Connection Manager LUA Host Object
{BA677074-762C-444b-94C8-8C83F93F6605}    User hive background upload task handler
{BA7C0D29-81CA-4901-B450-634E20BB8C34}    CPrintTicket WoW Services
{ba818ce5-b55f-443f-ad39-2fe89be6191f}    Function Instance Collection Class
{BAA94581-C092-425C-B4D3-7B5EE0BAC3C4}    Windows Media Player WMEncProfile2 Class
{BAEA8DC9-45F5-4DF8-A27F-2A277D524B15}    WIA Extension Host for 64 bit extensions
{BB07BACD-CD56-4E63-A8FF-CBF0355FB9F4}    EventSystem.EventObjectChange2
{BB18C7A0-2186-4be0-97D8-04847B628E02}    WpcProviderSupport Class
{BB2D41DF-7E34-4F06-8F51-007C9CAD36BE}    WlanAdhoc LUA
{BB44391D-6ABD-422f-9E2E-385C9DFF51FC}    DxtCompositor Class
{BB530C63-D9DF-4B49-9439-63453962E598}    Encoder Feature Segment
{BB64F8A7-BEE7-4E1A-AB8D-7D8273F7FDB6}    Action Center CPL
{bb6df56b-cace-11dc-9992-0019b93a3a84}    Background Intelligent Transfer Control
Class 4.0
{BB847B8A-054A-11d2-A894-0000F8084F96}    CLSID_IPropFindRequest
{BB89EB37-081E-4F5D-BA35-8D636BB47440}    MSASR Locale Handler Class (1028)
{bbb5d0e2-6f4b-4c31-8744-22d0029c4b40}    Function Discovery Print Provider
{BBC40082-8ABB-4DDD-B1C6-4EE0A9A5DB52}    WMPlayer PlaylistPropPage Class
{BBEC4F81-C2BC-43a7-BD95-9738EE9B6CCA}    WMPlayer DVDPropPage Class
{bbeea841-0a63-4f52-a7ab-a9b3a84ed38a}    MP3 Decoder DMO
{BC08386A-9952-40CD-BA50-9541D64A4B4E}    PSFactoryBuffer
{BC271022-28CD-468A-BBB0-EF7091D8625E}    Connecting Progress Page Class
{BC29A660-30E3-11D0-9E69-00C04FD7C15B}    WDM Streaming VPE Property Set Interface
Handler
{BC48B32F-5910-47F5-8570-5074A8A5636A}    Sync Results Delegate Folder
{BCA2CD56-422C-44F8-B3F4-A1B7885AC007}    EnumSTSWORDEDIT Class
{BCDE0395-E52F-467C-8E3D-C4579291692E}    MMDeviceEnumerator class
{BD0D38E4-74C8-4904-9B5A-269F8E9994E9}    ImageProcess Class
{BD4F77B3-70B0-4464-83A5-785F205B823B}    InkTablet Class
{BD6EDFCA-2890-482F-B233-8D7339A1CF8D}
{BD70C020-2D24-11D0-9110-00004C752752}
{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}    @%systemroot%\system32\mssvp.dll,-112
{bde9ee7c-329f-4fcf-ba7a-f8c6e9b4579d}    DUI Shell View Frame
{BDF23680-C1E5-11D2-9EF7-006008039E37}    Pin Property
{BDFEE05A-4418-11DD-90ED-001C257CCFF1}    Mbn ConnectionProfile Manager
{BDFEE05B-4418-11DD-90ED-001C257CCFF1}    Mbn Interface Manager
{BDFEE05C-4418-11DD-90ED-001C257CCFF1}    Mbn Connection Manager
{BE09F473-7FEB-11d2-9962-00C04FA309D4}    CLSID_MigrateMessageStore
{BE8E0170-72DC-11D2-952A-0060081840BC}    Stretch Property Page
{BF27441E-CDCD-4659-AEBE-06F6E069714E}    Screen Capture Filter Task Page
{bf29a3a2-d2bf-4a22-96cc-9aceb0f94cba}    Policy for Glass tree item callback object
for sysdm.cpl
{bf50b68e-29b8-4386-ae9c-9734d5117cd5}    IShellFolder marshaler app compat stub
{BF5CB148-7C77-4d8a-A53E-D81C70CF743C}    AD RMS Rights Policy Template Management
(Manual) Task Handler
{bf641d1c-29fd-4721-b3b8-48d92d35f7df}    CLSID_QueryFactoryWithOptions
{BF87B6E0-8C27-11D0-B3F0-00AA003761C5}    Capture Graph Builder
{BF87B6E1-8C27-11D0-B3F0-00AA003761C5}    Capture Graph Builder 2
{BF981FDD-B743-11D1-A69A-00C04FB9988E}    MachineSettings Class
{BFCB2C6D-04AA-4fb9-BC72-58E1AF64BE39}    Nap Server Management class
{BFD468D2-D0A0-4bdc-878C-E69C2F5B435D}    CLSID_PreviewUrl
{BFD6C433-4B17-4F6D-A93C-B03FCC4E586E}    WPD PnPX Association Manager Class
{BFE18E9C-6D87-4450-B37C-E02F0B373803}    AutomaticUpdates Class
{C01B9BA0-BEA7-41BA-B604-D0A36F469133}    SystemInformation Class
{C03E8500-781E-49a1-8190-CE902D0B2CE7}    Connection to work options Page
{C03E8511-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup CTI Hook Page (non-UI)
{C03E8512-781E-49a1-8190-CE902D0B2CE7}    Dialup CTI Connection Retry Page
{C03E8513-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup Connection Info Page
{C03E8521-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup CTW Hook Page (non-UI)
{C03E8522-781E-49a1-8190-CE902D0B2CE7}    Dialup CTW Connection Retry Page
{C03E8523-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup (CTW) Connection Info Page
```

Page 88

SOFTWARE OUTPUT.txt

```
{C03E8524-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup (CTW) User Info Page
{C03E8531-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Check Internet Connection
{C03E8532-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Hook Page (non-UI)
{C03E8533-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Connection Info Page
{C03E8534-781E-49a1-8190-CE902D0B2CE7}    RAS VPN User Info Page
{C03E8541-781E-49a1-8190-CE902D0B2CE7}    RAS PPPoE Hook Page (non-UI)
{C03E8542-781E-49a1-8190-CE902D0B2CE7}    RAS PPPoE Connection Info Page
{C03E8551-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Check Devices Page
{C03E8552-781E-49a1-8190-CE902D0B2CE7}    RAS Incoming Connection Hook Page (non-UI)
{C03E8553-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Users Page
{C03E8554-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Devices Page
{C03E8555-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Network Page
{C03E8556-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Save Page
{C03E8557-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Summary Page
{C03E8561-781E-49a1-8190-CE902D0B2CE7}    RAS New Connections Page
{C03E8565-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Work Testing Page Class
{C03E8566-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Internet Testing Page
Class
{C03E8568-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Work Finish Page Class
{C03E8569-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Internet Finish Page
Class
{C03E8571-781E-49a1-8190-CE902D0B2CE7}    VANUI RAS Connect Page Class
{C03E8572-781E-49a1-8190-CE902D0B2CE7}    VANUI RAS Disconnect Page Class
{C03E8581-781E-49a1-8190-CE902D0B2CE7}    Set up a new connection
{C03E8582-781E-49a1-8190-CE902D0B2CE7}    Set up a new virtual network connection
(VPN)
{C03E8583-781E-49a1-8190-CE902D0B2CE7}    Set up a new dialup connection
{C03E8584-781E-49a1-8190-CE902D0B2CE7}    Set up a new dialup connection (Internet)
{C03E8585-781E-49a1-8190-CE902D0B2CE7}    Set up a new broadband connection
{C03E8586-781E-49a1-8190-CE902D0B2CE7}    Incoming Connections Task Class
{C03E8591-781E-49A1-8190-CE902D0B2CE7}    XWizard Factory Generated Class
{C03E8592-781E-49A1-8190-CE902D0B2CE7}    XWizard Factory Generated Class
{c047c5a9-c407-4a1e-ad7f-11d0861344b7}    L2Sec Helper Class
{c04b329e-5823-4415-9c93-ba44688947b0}
{C04D65CF-B70D-11D0-B188-00AA0038C969}    Multi Language String
{C0A4145B-E627-40E3-AECC-FD392DC9B959}    XWizard Factory Generated Class
{C0B35746-EBF5-11D8-BBE9-505054503030}    PSFactoryBuffer
{C0B3C446-3032-4016-926F-9BAE48BEBFBE}    IMOfferRA Class
{C0B4E2F3-BA21-4773-8DBA-335EC946EB8B}    File Save Dialog
{C0BC4B4A-A406-4EFC-932F-B8546B8100CC}    UPnPServices Class
{C0E13E61-0CC6-11d1-BBB6-0060978B2AE6}    Data Driven Cleaner
{C100BE9A-D33A-4a4b-BF23-BBEF4663D017}    WCN Discovery Provider Class
{C100BEA3-D33A-4a4b-BF23-BBEF4663D017}    WCN Discovery Object
{C100BEB7-D33A-4a4b-BF23-BBEF4663D017}    WCN Autorun Handler
{C100BEBB-D33A-4a4b-BF23-BBEF4663D017}    WCN Elevation Helper
{C100BEBC-D33A-4a4b-BF23-BBEF4663D017}
{C100BED0-D33A-4a4b-BF23-BBEF4663D017}
{C100BED1-D33A-4a4b-BF23-BBEF4663D017}
{C100BED3-D33A-4a4b-BF23-BBEF4663D017}
{C100BED4-D33A-4a4b-BF23-BBEF4663D017}
{C100BED7-D33A-4a4b-BF23-BBEF4663D017}
{C100BED9-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDA-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDB-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDC-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDD-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDE-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE1-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE2-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE3-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE5-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE6-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE7-D33A-4a4b-BF23-BBEF4663D017}
```

Page 89

SOFTWARE OUTPUT.txt

```
{C100BEE9-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEA-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEB-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEC-D33A-4a4b-BF23-BBEF4663D017}
{C100BEED-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEE-D33A-4a4b-BF23-BBEF4663D017}
{C100BEF0-D33A-4a4b-BF23-BBEF4663D017}
{C100BEF1-D33A-4a4b-BF23-BBEF4663D017}
{C100BEF2-D33A-4a4b-BF23-BBEF4663D017}
{C100BEF3-D33A-4a4b-BF23-BBEF4663D017}
{C10B4771-4DA0-11D2-A2F5-00C04F86FB7D}    Winmgmt MOF Compiler
{C120DE80-FDE4-49f5-A713-E902EF062B8A}    MF MP3 Property Handler
{c1243ca0-bf96-11cd-b579-08002b30bfeb}    Plain Text filter
{C1282A7B-9455-48dc-BBBB-46C2EB525AF5}    WMPlayer VizResolutionPropPage Class
{c15e6bf0-6351-4588-ac4f-ef7d5ec8c16e}    WMPlayer LibraryPropPage Class
{C169CC11-1EC1-4847-9C0D-D2F2D80D07CF}    Microsoft WBEM Smart Object Marshaler
{C19FBD0E-7663-44ea-8265-74130671A1D6}    OpenSearch Description Location Creator
{C1F400A0-3F08-11D3-9F0B-006008039E37}    Sample Grabber
{C1F400A4-3F08-11D3-9F0B-006008039E37}    Null Renderer
{c1f85ef8-bcc2-4606-bb39-70c523715eb3}    ScheduledDiagnosticCustomHandler
{C20447FC-EC60-475E-813F-D2B0A6DECEFE}    Extensible Eventing Service
{c206f324-bb45-4765-93ff-3bca7306ff2e}    CommonLayoutDefinition
{C20CE506-5DA9-4B9C-9662-D88BD30E10A1}    PrinterQueueViewJobExtension Class
{C228A457-53F5-4a76-8035-DF2DA33E76C8}
{C2566514-DD44-4c6c-AAAD-FBD2F18D8DEE}    Property Set Storage In Memory Object
{c278aba7-cc1c-4717-bdfb-db2bca78246e}    Grouping Helper Class
{C2796011-81BA-4148-8FCA-C6643245113F}    Network Tray SSO
{c2d2c3a4-9a7e-11da-8bf7-0007e95ead8d}    SBF File
{C2DAE44D-C850-425c-B466-D8CBC1469F5D}
{C2E88C2F-6F5B-4AAA-894B-55C847AD3A2D}    WindowsUpdateAgentInfo Class
{C2FBB630-2971-11d1-A18C-00C04FD75D13}    Microsoft CopyTo Service
{C2FBB631-2971-11d1-A18C-00C04FD75D13}    Microsoft MoveTo Service
{c3278e90-bea7-11cd-b579-08002b30bfeb}    Null filter
{C3701884-B39B-11D1-9D68-00C04FC30DF6}    OleInstall Class
{C39E156D-F621-48CF-B0EE-9C47C430543B}    Windows Media Player
WMEncFileTransferSourcePropertyPage Class
{C4050BC4-29E1-4c8f-BF6E-6EBAD21E0673}    HomeGroup Printer Monitor
{C40FBD00-88B9-11d2-84AD-00C04FA31A86}
{C424F25A-6774-48BC-9F1E-02CCA8C1BE62}    Troubleshooting Control Panel
{C447080C-D0C3-48AE-B31E-BB3E93591C69}    WMEnc DV Timecode Reader
{C45268A2-FA81-4E19-B1E3-72EDBD60AEDA}    MSVidCtl Enhanced Video Renderer(DX10)
Segment
{c463a0fc-794f-4fdf-9201-01938ceacafa}    RasMobilityManager
{C47195EC-CD7A-11D1-8EA3-00C04F9900D7}    SysColorCtrl class
{c472004d-44fb-41e9-ac0a-7b920384a850}    Device Center Print Commands Extension
{C47A41B7-B729-424f-9AF9-5CB3934F2DFA}    WinSAT Query OEM Customization Object
{C49E32C6-BC8B-11d2-85D4-00105A1F8304}    Windows Management Instrumentation Backup
and Recovery
{c4bbedb4-e9b9-4e41-8fe1-0786480a2173}    CL2TPDiagHelper Object
{C4BF2784-AE00-41BA-9828-9C953BD3C54A}    MSVidCtl CC to Video Renderer Composition
Segment
{C4C4C481-0049-4E2B-98FB-9537F6CE516D}    Encrypt
{C4C4C482-0049-4E2B-98FB-9537F6CE516D}    Decrypt
{C4C4C483-0049-4E2B-98FB-9537F6CE516D}    Properties
{C4C4C491-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C492-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C493-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C4F1-0049-4E2B-98FB-9537F6CE516D}    Encrypt/Tag
{C4C4C4F2-0049-4E2B-98FB-9537F6CE516D}    Decrypt/Tag
{C4C4C4F3-0049-4E2B-98FB-9537F6CE516D}    XDS Codec
{C4C4C4FC-0049-4E2B-98FB-9537F6CE516D}
{C4D81942-0607-11D2-A392-00E0291F3959}    Big Switch
{C4D81943-0607-11D2-A392-00E0291F3959}    Smart Recompressor
```

Page 90

```
                          SOFTWARE  OUTPUT.txt
{C4EC38BD-4E9E-4b5e-935A-D1BFF237D980}   Explorer Travel Band
{c51b83e5-9edd-4250-b45a-da672ee3c70e}   Restore Default Libraries Command
{C529C7EF-A3AF-45F2-8A47-767B33AA5CC0}   Network Diagnostics Framework
{C52FF1FD-EB6C-42CF-9140-83DEFECA7E29}   InkObjectXP Class
{C531D9FD-9685-4028-8B68-6E1232079F1E}   BDA Tuning Model DVB Cable Locator
{C5599E1B-FC7B-4883-9FF4-581BBAEF8DBA}   Bluetooth FD Provider Proxy
{C5702CCC-9B79-11D3-B654-00C04F79498E}   Input Devices Collection Class
{C5702CCD-9B79-11D3-B654-00C04F79498E}   Output Devices Collection Class
{C5702CCE-9B79-11D3-B654-00C04F79498E}   Video Renderers Collection Class
{C5702CCF-9B79-11D3-B654-00C04F79498E}   Audio Renderers Collection Class
{C5702CD0-9B79-11D3-B654-00C04F79498E}   Features Collection Class
{C5702CD6-9B79-11D3-B654-00C04F79498E}   Custom Composition Segment from Legacy
Analog Tv Tuner Device Segment to Data Services Feature Segment
{c57a6066-66a3-4d91-9eb9-41532179f0a5}   AppSuggestedLocations
{C58C4893-3BE0-4B45-ABB5-A63E4B8C8651}   Troubleshooting
{c5a40261-cd64-4ccf-84cb-c394da41d590}   Video Thumbnail Extractor
{C5B19592-145E-11d3-9F04-006008039E37}   DxtKey Class
{C5B56EA1-5853-3310-B3E2-924E9F0BA355}
{C5C5C5F0-3ABC-11D6-B25B-00C04FA0C026}   XDSToRat Class
{C5C5C5F1-3ABC-11D6-B25B-00C04FA0C026}   EvalRat Class
{C605507B-9613-4756-9C07-E0D74321CB1E}   CLSID_HomeGroupCtrl
{C61BFCDF-2E0F-4AAD-A8D7-E06BAFEBCDFE}
{C624BA95-FBCB-4409-8C03-8CCEEC533EF1}   UPnPService Class
{c63382be-7933-48d0-9ac8-85fb46be2fdd}   Default Folder Menu
{C647B5C0-157C-11D0-BD23-00A0C911CE86}   AVI mux Property Page
{C64B9B66-E53D-4c56-B9AE-FEDE4EE95DB1}   Condition History Class
{C666E115-BB62-4027-A113-82D643FE2D99}   MPEG-2 Sections and Tables
{C68411EA-1396-48f3-AF98-B7F657E35C20}   Autoplay Device Handler
{C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7}   BDA Tuning Model DVB Tuning Space
{C6B400E2-20A7-4E58-A2FE-24619682CE6C}   Microsoft AC3 Encoder
{C6B5F214-0743-3868-B1EA-C4C23CE2AF52}
{C6CC49B0-CE17-11D0-8833-00A0C903B83C}   CertGetConfig Class
{C6E13343-30AC-11D0-A18C-00A0C9118956}   IAMVideoCompression
{C6E13344-30AC-11D0-A18C-00A0C9118956}   IAMDroppedFrames
{C6E13350-30AC-11D0-A18C-00A0C9118956}   IAMAnalogVideoDecoder
{C6E13360-30AC-11D0-A18C-00A0C9118956}   IAMVideoProcAmp
{C6E13370-30AC-11D0-A18C-00A0C9118956}   IAMCameraControl
{C707F6A6-A1F3-45d7-99AA-A2B9491E84AD}   CLSID_PublicationServices
{C71566F2-561E-11D1-AD87-00C04FD8FDFF}   Microsoft WBEM Universal Refresher
{C72BE2EC-8E90-452c-B29A-AB8FF1C071FC}   FunctionDiscovery Class
{c73f6f30-97a0-4ad1-a08f-540d4e9bc7b9}   CLSID_AutoListPropertyStore
{c79d1575-b8c6-4862-a284-788836518b97}   Windows Display Settings
{C7B6C04A-CBB5-11d0-BB4C-00C04FC2F410}   IndexServer Simple Command Creator
{C7CA6167-2F46-4C4C-98B2-C92591368971}   New Library Menu Handler
{c827f149-55c1-4d28-935e-57e47caed973}   Shell Web Wizard Host Object
{C8B522CF-5CF3-11CE-ADE5-00AA0044773D}   Microsoft OLE DB Error Collection Service
{c8b522d0-5cf3-11ce-ade5-00aa0044773d}   Microsoft OLE DB Root Enumerator
{c8b522d1-5cf3-11ce-ade5-00aa0044773d}   Microsoft OLE DB Data Conversion Library
{c8c97725-c948-4720-bf0f-e3c2273bfb7d}   Library Initialization Handler
{c8e6f269-b90a-4053-a3be-499afcec98c4}   User Account Control Check Provider
{C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6}   PSFactoryBuffer
{c9298eef-69dd-4cdd-b153-bdbc38486781}   State of verb Empty Recycle Bin
{C96401CC-0E17-11D3-885B-00C04F72C717}   Folder
{C96401CF-0E17-11D3-885B-00C04F72C717}   OCX
{C96401D1-0E17-11D3-885B-00C04F72C717}   HTML
{C9A14CDA-C339-460B-9078-D4DEBCFABE91}
{C9D849E0-FBF6-4C26-B1EC-B5D5B4E3F29D}   Microsoft MPEG-2 Audio Encoder Property
Page
{C9F5FE02-F851-4EB5-99EE-AD602AF1E619}   StreamBufferSource
{CA22F5B1-E06F-4A2B-94FC-21E87FE53781}   GameUpdateTask Class
{CA2AF3B4-C15E-412b-B453-557746675FB7}   WmiPerf Instance Provider
{ca34fe0a-5722-43ad-af23-05f7650257dd}   ADPCM ACM Wrapper MFT
{CA38D8DA-C75D-11D1-8F99-00600895E7D5}   Interface Proxy Stub
                          Page 91
```

```
                         SOFTWARE OUTPUT.txt
   {CA38D8DB-C75D-11D1-8F99-00600895E7D5}   Interface Proxy Stub
   {CA3FDCA2-BFBE-4eed-90D7-0CAEF0A1BDA1}   PSFactoryBuffer
   {CA81B096-1D6F-4635-956E-F08C0B2EC342}   Windows Media Player WMEncImageSource
Class
   {CAAFDD83-CEFC-4E3D-BA03-175F17A24F91}   Stream Buffer Recording Control Object
   {CACAF262-9370-4615-A13B-9F5539DA4C0A}
   {CAE80521-F685-11d1-AF32-00C04FA31B90}   CLSID_OENote
   {CB0FC8E5-686A-478B-A252-FDECF8E167B7}   scanprofilemgr class
   {CB17E772-E1CC-4633-8450-5617AF577905}
   {CB1B7F8C-C50A-4176-B604-9E24DEE8D4D1}   Getting Started
   {CB1DFE3A-EDFF-4d1f-867D-8ADB02926F4B}   OpenSearch Description Create Search
Connector Verb Handler
   {CB2F6723-AB3A-11d2-9C40-00C04FA30A3E}   Microsoft Common Language Runtime Meta
Data
   {CB39A782-E5E4-11D1-8CC0-00C04FC3261D}   RegDBCompensator Class
   {CB46E850-FC2F-11D2-B126-00805FC73204}   PSFactoryBuffer
   {CB8555CC-9128-11D1-AD9B-00C04FD8FDFF}   WbemAdministrativeLocator Class
   {CB8C13E4-62B5-4C96-A48B-6BA6ACE39C76}
  .{cba9e78b-49a3-49ea-93d4-6bcba8c4de07}   Mpeg43 Decoder DMO
   {CBC84B69-69EA-439B-B791-DF15F60333CF}   Biometrics navigate target object
   {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E}   TV: Pluggable Protocol
   {CBD51D89-C22E-4388-A553-FFE638C76E36}
   {CC1101F2-79DC-11D2-8CE6-00A0C9441E20}   MediaLocator Class
   {CC19079B-8272-4D73-BB70-CDB533527B61}   HNetCfg.FwProducts
   {CC23F537-18D4-4ECE-93BD-207A84726979}   MSVidCtl FilePlayback to Audio Renderer
Composition Segment
   {CC48A47F-EFD6-4925-A515-28C40C5A78B6}   MSASR Locale Handler Class (1041)
   {CC58E280-8AA1-11D1-B3F1-00AA003761C5}   Smart Tee Filter
   {CC58E281-8AA1-11D1-B3F1-00AA003761C5}   DirectX Transform Wrapper
   {cc5bbec3-db4a-4bed-828d-08d78ee3e1ed}   JScript Compact Profile (ECMA 327)
   {CC6EEFFB-43F6-46c5-9619-51D571967F7D}   Web Publishing Wizard
   {CC785860-B2CA-11CE-8D2B-0000E202599C}   MPEG Audio Decoder Property Page
  .{CC7BFB42-F175-11d1-A392-00E0291F3959}   Video Effect (1 input) Class Manager
   {CC7BFB43-F175-11d1-A392-00E0291F3959}   Video Effect (2 input) Class Manager
   {CC829A2F-3365-463F-AF13-81DBB6F3A555}   BDA Tuning Model Channel ID Tuning Space
   {CC9072AB-C000-49D8-A5AA-00266C8DBB9B}   Microsoft WBEM _IWbemEnumMarshaling
Enumerator Helper
   {CCAA63AC-1057-4778-AE92-1206AB9ACEE6}   StreamBufferRecordingAttributes
   {CCB4EC60-B9DC-11D1-AC80-00A0C9034873}   PDPO Class
   {CCDEDADE-AE23-47f3-A588-B09A05CA1A00}   DcpSearchTargetServices
   {CCFB7955-B4DC-42CE-893D-884D72DD6B19}   Biometrics navigate target object
   {CD12A3CE-9C42-11D2-BEED-0060082F2054}   ClientNetManager Class
   {CD184336-9128-11D1-AD9B-00C04FD8FDFF}   WbemAuthenticatedLocator Class
   {CD1ABFC8-6C5E-4A8D-B90B-2A3B153B886D}   Microsoft WBEM
_IWbemConfigureRefreshingSvc Configure Refreshing Services Factory
   {cd3aa379-93f4-421b-9802-aeab68b06771}   RdpVideoSink Class
   {CD3AFA70-B84F-48F0-9393-7EDC34128127}   APPLICATION__X_MPLAYER2 Moniker Class
   {CD3AFA71-B84F-48F0-9393-7EDC34128127}   APPLICATION__X_MS_WMZ Moniker Class
   {CD3AFA72-B84F-48F0-9393-7EDC34128127}   AUDIO__AIFF Moniker Class
  .{CD3AFA73-B84F-48F0-9393-7EDC34128127}   AUDIO__BASIC Moniker Class
   {CD3AFA74-B84F-48F0-9393-7EDC34128127}   AUDIO__MID Moniker Class
   {CD3AFA76-B84F-48F0-9393-7EDC34128127}   AUDIO__MP3 Moniker Class
   {CD3AFA77-B84F-48F0-9393-7EDC34128127}   AUDIO__MPEG Moniker Class
   {CD3AFA78-B84F-48F0-9393-7EDC34128127}   AUDIO__MPEGURL Moniker Class
   {CD3AFA7A-B84F-48F0-9393-7EDC34128127}   AUDIO__SCPLS Moniker Class
   {CD3AFA7B-B84F-48F0-9393-7EDC34128127}   AUDIO__WAV Moniker Class
   {CD3AFA7C-B84F-48F0-9393-7EDC34128127}   AUDIO__MP4 Moniker Class
   {CD3AFA7D-B84F-48F0-9393-7EDC34128127}   AUDIO__VND_DLNA_ADTS Moniker Class
   {CD3AFA83-B84F-48F0-9393-7EDC34128127}   AUDIO__X_MS_WAX Moniker Class
   {CD3AFA84-B84F-48F0-9393-7EDC34128127}   AUDIO__X_MS_WMA Moniker Class
   {CD3AFA88-B84F-48F0-9393-7EDC34128127}   VIDEO__AVI Moniker Class
   {CD3AFA89-B84F-48F0-9393-7EDC34128127}   VIDEO__MPEG Moniker Class
   {CD3AFA8F-B84F-48F0-9393-7EDC34128127}   VIDEO__X_MS_ASF Moniker Class
                               Page 92
```

SOFTWARE OUTPUT.txt

```
{CD3AFA90-B84F-48F0-9393-7EDC34128127}    VIDEO__X_MS_ASF_PLUGIN Moniker Class
{CD3AFA92-B84F-48F0-9393-7EDC34128127}    VIDEO__X_MS_WM_ Moniker Class
{CD3AFA93-B84F-48F0-9393-7EDC34128127}    VIDEO__X_MS_WMX Moniker Class
{CD3AFA94-B84F-48F0-9393-7EDC34128127}    VIDEO__X_MS_WMV Moniker Class
{CD3AFA95-B84F-48F0-9393-7EDC34128127}    VIDEO__X_MS_WVX Moniker Class
{CD3AFA96-B84F-48F0-9393-7EDC34128127}    APPLICATION__X_WMPLAYER Moniker Class
{CD3AFA97-B84F-48F0-9393-7EDC34128127}    AUDIO__3GPP Moniker Class
{CD3AFA98-B84F-48F0-9393-7EDC34128127}    AUDIO__3GPP2 Moniker Class
{CD3AFA99-B84F-48F0-9393-7EDC34128127}    VIDEO__MP4 Moniker Class
{CD3AFA9A-B84F-48F0-9393-7EDC34128127}    VIDEO__QUICKTIME Moniker Class
{CD3AFA9B-B84F-48F0-9393-7EDC34128127}    AUDIO__VND_MPEG_TTS Moniker Class
{cd4b7782-eb37-4bfe-b9ce-685f634a08dc}    CSdwhcNotifier Class
{CD5096A1-E7E7-4E09-8B12-CBF2790A87CF}    Bluetooth Personal Area Connection
Enumerator
{CD6C7868-5864-11D0-ABF0-0020AF6B0B7A}    CTreeView Control
{CDA42200-BD88-11D0-BD4E-00A0C911CE86}    Filter Mapper2
{CDBD8D00-C193-11D0-BD4E-00A0C911CE86}    CMediaPropertyBag
{CDBEC9C0-7A68-11D1-88F9-0080C7D771BF}    Event Class
{cdc32574-7521-4124-90c3-8d5605a34933}    Windows Media Player Burn Audio CD Handler
{CDC82860-468D-4d4e-B7E7-C298FF23AB2C}    ShellItemArray Shell Namespace helper
{CE39D6F3-DAB7-41b3-9F7D-BD1CC4E92399}    WCF/COM+ Integration Service Moniker
{CE69CC1E-1EC0-4847-9C0D-D2F2D80D07CF}    Microsoft WBEM Message Service
{ceefea1b-3e29-4ef1-b34c-fec79c4f70af}    New Shortcut Wizard
{ceff45ee-c862-41de-aee2-a022c81eda92}    CLSID_SeparateSingleProcessExplorerHost
{CF1BF3B6-7AD0-4410-996B-C78EAFCD3269}    Windows Markup File
{CF2CF428-325B-48d3-8CA8-7633E36E5A32}    AD RMS Rights Policy Template Management
(Automated) Task Handler
{CF49D4E0-1115-11CE-B03A-0020AF0BA770}    AVI Decompressor
{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}    WbemDefaultPathParser
{CF67796C-F57F-45f8-92FB-AD698826C602}    .contact shell context menu
{cfb16474-0a2e-48dc-88ce-8c0adb7e5e46}    Windows Media Player Device Options
Property Page
{cfbc05bc-1b9e-4693-a49c-4e7181d69e0a}    Windows Update Control Panel
{CFC399AF-D876-11D0-9C10-00C04FC99C8E}    Msxml
{CFCCC7A0-A282-11D1-9082-006008059382}    Darwin App Publisher
{CFF9990B-6414-43F1-A526-14EA5EEAFBDA}    Library Share Engine
{D02AAC50-027E-11D3-9D8E-00C04F72D980}    Collection of all the available BDA Tuning
Model Tuning Space objects on this system
{D032FDC6-3736-4AF0-BE08-6F6E52979BBD}    New Network category Status Page
{D049B20C-5DD0-44FE-B0B3-8F92C8E6D080}
{D0565000-9DF4-11D1-A281-00C04FCA0AA7}    EventSystem.EventObjectChange
{d0b7e02c-e1a3-11dc-81ff-001185ae5e76}    DiagnosticProfile
{D0E55F9F-0021-42fe-A1DB-C41F5B564EFE}    RASMapi Class
{D13E3F25-1688-45A0-9743-759EB35CDF9A}    AcquisitionManager Class
{D1621129-45C4-41AD-A1D1-AF7EAFABEEDC}    WIA Default UI
{D169C14A-5148-4322-92C8-754FC9D018D8}    rtf persistent handler for mapi email
{D16B87DE-029E-4C85-92C8-ED8BBC5E882C}    Microsoft Embedded Search Gatherer Inline
Notification
{d1a42999-0adf-11da-b070-0011856571de}
{d1a4299a-0adf-11da-b070-0011856571de}
{D20EA4E1-3957-11d2-A40B-0C5020524153}    Administrative Tools
{D215781D-019E-4FA0-903D-0CDCDE13A4F5}    Winmgmt MOF Compiler OOP
{d23b90d0-144f-46bd-841d-59e4eb19dc59}    WMVideo9 Encoder DMO
{D2423620-51A0-11D2-9CAF-0060B0EC3D39}    XML Parser
{D26AA4A5-92AD-48DB-8D59-95EF0DCE6939}    CMigrationPlugin Object
{D2AC2892-B39B-11D1-8704-00600893B1BD}    DirectMusicLoader
{D2E0FE7F-D23E-48E1-93C0-6FA8CC346474}    UpdateInstaller Class
{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}    ColorDataProxy
{D2ED260C-38F1-4ABE-8B2B-D4A088C54416}    PSFactoryBuffer
{D31B6A3F-9350-40DE-A3FC-A7EDEB9B7C63}    WMI instrumentation:
Win32_SystemConfigurationChangeEvent
{d34a6ca6-62c2-4c34-8a7c-14709c1ad938}    Common Places FS Folder
{D34BD150-6D84-443E-83EE-04C7682377E4}    Unsecured Net Connect Control Class
```

Page 93

```
                          SOFTWARE OUTPUT.txt
{D3588AB0-0781-11CE-B03A-0020AF0BA770}   AVI/WAV File Source
{D39E7BDD-7D05-46b8-8721-80CF035F57D7}   CivicAddress Report Class
{D3C536B8-D0EC-48AB-838F-D4CC9A281BB5}   STSServerInstance Class
{d3c86d56-03a1-42d5-af4c-1b612be90448}   CLSID_TryHarderItemFactory
{D4480A50-BA28-11d1-8E75-00C04FA31A86}   Add Network Place
{d450a8a1-9568-45c7-9c0e-b4f9fb4537bd}   Installed Updates
{D4692569-5A04-351D-8BA7-5F43AB458DF6}   `
{D4DCD3D7-B4C2-47D9-A6BF-B89BA396A4A3}
{d4f01ada-979c-491e-bac3-cd3c0e7bcf82}   Online Id Filter
{D4F4D30B-0B29-4508-8922-0C5797D42765}   WIA Default Segmentation Filter
{D51BD5A1-7548-11CF-A520-0080C77EF58A}   Wave Parser
{D51BD5A2-7548-11CF-A520-0080C77EF58A}   MIDI Parser
{D51BD5A3-7548-11CF-A520-0080C77EF58A}   Multi-file Parser
{D51BD5A5-7548-11CF-A520-0080C77EF58A}   File stream renderer
{D5307D61-F9BC-4de1-94EA-1DEF24DF4BB2}
{d54378cd-91d8-4e10-a00b-819f9a9efcb1}   CoFilterPipeline Class
{D5753BBB-C5A8-4F50-9D81-210BAB0C5FB6}   Mpeg-2 Stats
{d58960ba-2ef3-4910-9e34-c911b1710180}   ShellTravelLog
{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}   SENS Network Events
{D5978630-5B9F-11D1-8DD2-00AA004ABD5E}   SENS Logon Events
{D5978640-5B9F-11D1-8DD2-00AA004ABD5E}   SENS OnNow Events
{D5978650-5B9F-11D1-8DD2-00AA004ABD5E}   SENS Logon2 Events
{D5C66BE1-C209-11d1-8DEC-00C04FC2E0C7}
{D5ED6B03-EDA3-4cbc-9FF1-60182438C8F6}   WSD Print Proxy Class
{D6015EC3-FA16-4813-9CA1-DA204574F5DA}   AlgController Class
{D6108DC8-FBAC-426e-8A3C-1BCA926E5805}   Enable transparent glass tree item
callback object for sysdm.cpl
{D63A1416-FCEC-4431-862F-E8056223DD03}   Windows Photo Viewer DropTarget
{D63A5850-8F16-11CF-9F47-00AA00BF345C}   WBEM Framework Instance Provider
{D63AA156-D534-4BAC-9BF1-55359CF5EC30}   Sync Center User Profile Notification
Handler
{D6564DE1-6163-3076-A8FB-D301CB439E30}
{D66949A0-C766-48D7-B2C6-4A85382BE9C1}   MSASR Locale Handler Class (3082)
{D66D6F99-CDAA-11D0-B822-00C04FC9B31F}   Multi Language ConvertCharset
{D6791A63-E7E2-4fee-BF52-5DED8E86E9B8}   Portable Devices Menu
{D682C4BA-A90A-42FE-B9E1-03109849C423}   StreamBufferComposeRecordingObj
{D68AF00A-29CB-43FA-8504-CE99A996D9EA}   Microsoft WBEM (non)Standard Marshaling
for IWbemServices
{D6EBC66B-8921-4193-AFDD-A1789FB7FF57}   PSFactoryBuffer
{D6F8EC75-A388-47de-BA3A-903B12A38E86}   PSFactoryBuffer
{D6FEDB1D-CF21-4BD9-AF3B-C5468E9C6684}   MMCVersionInfo 1.0 Object
{D707877E-4D9C-11d2-8784-F6E920524153}   User Property Pages
{D722AF63-6A0D-4e37-BD40-CF6FAC79A83C}   WMPDMCCoreServices Class
{D76334CA-D89E-4BAF-86AB-DDB59372AFC2}   MSVidCtl CC to Audio Renderer Composition
Segment
{D7B70EE0-4340-11CF-B063-0020AFC2CD35}   DirectDraw Object
{D7C1AEB5-10F2-48cb-A182-F7EF79C51B19}   WSD Publisher
{D8280A4F-FFED-3E98-8928-9F504A4A3361}
{D82BE2B0-5764-11D0-A96E-00C04FD705A2}   IShellFolderBand
{d84fa0c2-b0b3-4470-9345-75db0ec5a83a}   Universal Delegate Folder
{d851f103-8c90-4321-aff0-58ba5bd421c2}   SharedAccess Notification Sink
{D8559EB9-20C0-410E-BEDA-7ED416AECC2A}   Windows Defender
{D8872739-DF50-4ED5-B8A7-F03DCD0DCD5A}   PSFactoryBuffer
{D8BD090D-3F39-45FD-B29A-7FC62C2E59C3}   ExtTransport2 Class
{D8BF32A2-05A5-44c3-B3AA-5E80AC7D2576}   DrawingAttributes Class
{D8F0F5E7-11C5-4E95-BBFF-0F110C0221C4}
{d912f8cf-0396-4915-884e-fb425d32943b}   Property Helper Object
{D9403860-297F-4A49-BF9B-77898150A442}
{D94EDF02-EFE5-4F0D-85C8-F5A68B3000B1}
{D957171F-4BF9-4de2-BCD5-C70A7CA55836}   Interval Class
{D969A300-E7FF-11d0-A93B-00A0C90F2719}   New Menu Handler
{D978F0CB-DEBA-4388-83BE-D3E106E02A4F}   CardSpaceIETokenProvider Class
{d9b3211d-e57f-4426-aaef-30a806add397}   Shell Library API
```

                                   Page 94

SOFTWARE OUTPUT.txt
```
{D9BB4CEE-B87A-47F1-AC92-B08D9C7813FC}   BDA Tuning Model Digital Cable Tuning
Space
{D9F9C262-6231-11D3-8B1D-00C04FB6BD3D}   WM ASF Writer Properties
{DA4E3DA0-D07D-11d0-BD50-00A0C911CE86}   ActiveMovie Filter Categories
{DA67B8AD-E81B-4c70-9B91-B417B5E33527}   Windows Search Shell Service Object
{DAA92564-78C8-40A3-96D2-9115A76B8F29}   WPD Settings Completion Page Class
{DAC9F469-0C67-4643-9258-87EC128C5941}   SREngine Class
{DAFD8210-5711-4B91-9FE3-F75B7AE279BF}   DirectSoundGargleDMO
{db4f3fa7-5a08-4100-95de-b46df509b902}   Legacy View Available Networks Task Class
{DB5D1FF4-09D7-11D1-BB10-00C04FC9A3A3}   FILEMGMT 1.0 Object
{DB5D1FF5-09D7-11D1-BB10-00C04FC9A3A3}   SvcVwr 1.0 Object
{DBC85A2C-C0DC-4961-B6E2-D28B62C11AD4}   GameStatistics Class
{DC0C0FE7-0485-4266-B93F-68FBF80ED834}   Microsoft DVBC Network Provider
{DC1C5A9C-E88A-4dde-A5A1-60F82A20AEF7}   File Open Dialog
{DC7A02CD-2E47-406C-BA5A-B08EC00C4238}   MAPISendMailServer
{DC8A3F5A-92B9-4C38-A81F-296612813880}
{DC923725-0FDD-45E1-AE74-EA09182E739B}   Microsoft WBEM Wbem Token Cache
{DCB00C01-570F-4A9B-8D69-199FDBA5723B}   NetworkListManager
{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1}   speechtextservice class
{DCED8DB0-11A5-4b16-AB9D-4E28CA38C99F}   Advanced Configuration Dialog
{DCF33DF4-B510-439F-832A-16B6B514F2A7}   Microsoft WBEM _IWbemRefresherMgr
Refresher Cache Factory
{DD06A84F-83BD-4d01-8AB9-2389FEA0869E}   Dot11 AdHoc Manager
{DD313E04-FEFF-11d1-8ECD-0000F87A470C}   User Assist
{DD522ACC-F821-461A-A407-50B198B896DC}   HardwareDeviceNotif
{DD732BF4-B9A8-4f46-BA39-F4C010929F5F}
{DD75716E-B42E-4978-BB60-1497B92E30C4}   text persistent handler for mapi email
{DDC0EED2-ADBE-40b6-A217-EDE16A79A0DE}   GenericFilter
{DDE33513-774E-4BCD-AE79-02F4ADFE62FC}
{DDE5783A-88B9-11d2-84AD-00C04FA31A86}
{de2d022d-2480-43be-97f0-d1fa2cf98f4f}   PropertyKeyCollection Class
{DE3F3560-3032-41B4-B6CF-F703B1B95640}   Windows Search Service Profile Notify
Handler
{DE4874D1-FEEE-11d1-A0B0-00C04FA31A86}
{DE4874D2-FEEE-11d1-A0B0-00C04FA31A86}
{DE75D012-7A65-11D2-8CEA-00A0C9441E20}   DxtJpeg Class
{DE77BA04-3C92-4d11-A1A5-42352A53E0E3}   Home Group Member Status
{DE815B00-9460-4F6E-9471-892ED2275EA5}   RecoManager Class
{DE9C1288-0F09-40ff-BA84-7F19279FA74B}   Idenity Listener CLSID
{DECBDC16-E824-436e-872D-14E8C7BF7D8B}   RtpObject Class
{DF0B3D60-548F-101B-8E65-08002B2BD119}   PSSupportErrorInfo
{DF60686C-2941-4893-80C0-F13173B719D3}   HomeGroup State
{DFA14C43-F385-4170-99CC-1B7765FA0E4A}   WpcNotificationsMonitor
{DFD74844-990B-4410-9DA0-2848EFA85D14}   WMPlayer ClipPropPage Class
{DFFACDC5-679F-4156-8947-C5C76BC0B67F}   delegate folder that appears in Users
Files Folder
{E03E85B0-7BE3-4000-BA98-6C13DE9FA486}   ConditionFactory Class
{E05592E4-C0B5-11D0-A439-00A0C9223196}   Plug In Distributor: IKsQualityForwarder
{e0ca5340-4534-11cf-b952-00aa0051fe20}   HTML filter
{E0CBC546-8950-43DD-99A9-A418DB7DD0B5}   Could Not Connect Page Class
{E0F158E1-CB04-11d0-BD4E-00A0C911CE86}   WaveOut and DSound Class Manager
{E0FA581D-2188-11D2-A739-00C04FA377A1}   Provider Binder for DS OLE DB Provider
{E10A508F-1699-40ba-A0DD-9DEB2D4DCAC3}
{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}   PSIProfileNotify
{E137B0D0-7A93-11D2-8CEA-00A0C9441E20}   DxtJpegPP Class
{E13EF4E4-D2F2-11d0-9816-00C04FD91972}   Menu Site
{E16C0593-128F-11D1-97E4-00C04FB9618A}   Simple File-based Log
{E16C0594-128F-11D1-97E4-00C04FB9618A}   ARIES Log Recovery Engine
{E18AF75A-08AF-11D3-B64A-00C04F79498E}   Custom Composition Segment from Legacy
Analog Tv Tuner Device Segment to Standard Video Renderer Device Segment
{E1BA41AD-4A1D-418F-AABA-3D1196B423D3}   SDChangeObj Class
{E1C5D730-7E97-4D8A-9E42-BBAE87C2059F}   DeviceManager Class
{E1D0AB13-2FE6-4DF0-8917-ED80CF0FEF6B}
```
Page 95

SOFTWARE OUTPUT.txt

```
{E1DE74AD-C368-4104-ADB1-57D00577247A}   WLAN Media Manager
{E1F1A0B8-BEEE-490D-BA7C-066C40B5E2B9}   Microsoft DTV-DVD Audio Decoder
{E2085F28-FEB7-404A-B8E7-E659BDEAAA02}   UPnPDeviceFinder Class
{E20870E2-3AD1-4b64-87BE-5AD5F17A53F0}   rtf persistent handler for mapi email
{E211B736-43FD-11D1-9EFB-0000F8757FCD}
{e2183960-9d58-4e9c-878a-4acc06ca564a}   Microsoft DocProp Custom Draw Multi-Value
Property Control
{E23CE3EB-5608-4E83-BCEF-27B1987E51D7}
{E2448508-95DA-4205-9A27-7EC81E723B1A}   SBE2 Sink
{E2510970-F137-11CE-8B67-00AA00A3F1A6}   AVI mux
{E26B366D-F998-43ce-836F-CB6D904432B0}   RealTimeStylus Class
{E2A4E630-7AD8-44f0-B6EE-D36EA4C6EB94}   Network Diagnostics Client Interface
Wrapper
{e2b07466-5250-4fc2-8949-46bf91f8cad0}
{E2C6779C-B7DE-3311-8A5B-41922461E7C0}
{E2CBCB87-9C07-4523-A78F-061499C83987}   WMI instrumentation:
Win32_VolumeChangeEvent
{e2fb4720-f45f-4a3c-8cb2-2060e12425c3}   MF AVI Property Handler
{E302CB55-5F9D-41A3-9EF3-61827FB8B46D}   PSFactoryBuffer
{E30629D1-27E5-11CE-875D-00608CB78066}   Audio Renderer
{E30629D2-27E5-11CE-875D-00608CB78066}   Audio Capture Filter
{E3633C03-DF7A-41E0-B903-CC349A05E021}   PSFactoryBuffer
{E37A73F8-FB01-43dc-914E-AAEE76095AB9}   WTVFile Property Handler
{E37E2028-CE1A-4f42-AF05-6CEABC4E5D75}   Shell Icon Handler for Application
References
{E37EF07F-8266-448B-8059-C2B35BAFE0CF}   SnapinState Class
{e3a4e5ca-55b2-4a06-b1ab-8fbecc7bca4b}   Authentication UI Terminal Services Bump
Dialog
{E3D5D93C-1663-4A78-A1A7-22375DFEBAEE}   InkTransform Class
{e3e478d6-a2f2-4791-89a3-21f5c78dc3ec}   File enumerator helper
{E413D040-6788-4C22-957E-175D1C513A34}   Sync Center Conflict Delegate Folder
{E4206432-01A1-4BEE-B3E1-3702C8EDC574}   Line 21 Decoder 2
{E423AF7C-FC2D-11d2-B126-00805FC73204}   RemoteHelper Class
{E436EBB1-524F-11CE-9F53-0020AF0BA770}   System Clock
{E436EBB2-524F-11CE-9F53-0020AF0BA770}   Filter Mapper
{E436EBB3-524F-11CE-9F53-0020AF0BA770}   Filter Graph
{E436EBB5-524F-11CE-9F53-0020AF0BA770}   File Source (Async.)
{E436EBB6-524F-11CE-9F53-0020AF0BA770}   File Source (URL)
{E436EBB7-524F-11CE-9F53-0020AF0BA770}   IPersistMoniker Plug In Distributor
{E436EBB8-524F-11CE-9F53-0020AF0BA770}   Filter Graph no thread
{E44E5D18-0652-4508-A4E2-8A090067BCB0}   Default Programs command object for Start
menu
{e44e9428-bdbc-4987-a099-40dc8fd255e7}   Execute Unknown
{e46787a1-4629-4423-a693-be1f003b2742}   MF WAV Property Handler
{E474E05A-AB65-4f6a-827C-218B1BAAF31F}   MF Video Mixer
{e4796550-df61-448b-9193-13fc1341b163}   Property Store
{E4979309-7A32-495E-8A92-7B014AAD4961}   VMR ImageSync 9
{E4BCAC13-7F99-4908-9A8E-74E3BF24B6E1}   DirectSoundCapture 8.0 Object
{E573236F-55B1-4EDA-81EA-9F65DB0290D3}
{E598560B-28D5-46aa-A14A-8A3BEA34B576}   Windows Photo Viewer Video Verbs
{E5B4EAA0-B2CA-11CE-8D2B-0000E202599C}   MPEG Video Decoder Property Page
{E5B8E079-EE6D-4E33-A438-C87F2E959254}   Location Class
{E5CA59F5-57C4-4DD8-9BD6-1DEEEDD27AF4}   Microsoft InkEdit Control
{E5CB7A31-7512-11D2-89CE-0080C792E5D8}   Microsoft Common Language Runtime Meta
Data
{e60687f7-01a1-40aa-86ac-db1cbf673334}   SUSInternal Class 1.0
{E63DE750-3BD7-4BE5-9C84-6B4281988C44}   Windows Search Scope Rule
{E6442437-6C68-4f52-94DD-2CFED267EFB9}   CLSID_TrayDesktopBand
{E64CCC22-8E66-4822-9F2F-7FC385645A03}
{E69FD98D-7EBE-4C01-BFED-67B4E4616A49}   Browser Thread Handshake
{E70C92A9-4BFD-11d1-8A95-00C04FB951F3}   CLSID_StoreNamespace
{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435}   CCertProvider
{e755468c-02f5-4d96-8487-3be68ffe633a}   Elevated Object Factory Server Manager
```

Page 96

SOFTWARE OUTPUT.txt

```
{e760e244-abb3-4c3c-b925-0781c8ceb46c}
{E77026B0-B97F-4cbb-B7FB-F4F03AD69F11}   Tuning Model Xml Serialization Utility
{E7772804-3287-418E-9072-CF2B47238981}
{E77CC89B-7401-4c04-8CED-149DB35ADD04}   WindowsParentalControls Class
{E77E1B8B-ECF3-4af0-8B5E-EB13739D5344}
{E785DD9D-3F87-3679-BB58-A3A4C80F4256}
{E7B2FB72-D728-49B3-A5F2-18EBF5F1349E}   PSFactoryBuffer
{E7DE9B1A-7533-4556-9484-B26FB486475E}   Network Map
{e7ed314f-2816-4c26-aeb5-54a34d02404c}   KernelCeipCustomHandler
{E810CEE7-6E51-4cb0-AA3A-0B985B70DAF7}   StrokeBuilder Class
{E8140D53-6535-46a5-B8A1-DA6C571DA9B9}   Quarantine SoH Protocol constructor class
{E8167EE2-AB45-4BAA-BD03-12590436D789}   CLSID_COE7Import
{e82a2d71-5b2f-43a0-97b8-81be15854de8}   ShellLink for Application References
{E846F0A0-D367-11D1-8286-00A0C9231C29}
{E882F102-F626-49E9-BD68-CE2BE7E59EA0}   SoundRecorder WAV Dest
{E882F102-F626-49E9-BD68-CE2BE7E59EB0}   SoundRecorder Volume Watch
{E882F102-F626-49E9-BD68-CE2BE7E59EC0}   SoundRecorder Null Renderer
{E9495B87-D950-4ab5-87A5-FF6D70BF3E90}   Security Center
{E96767E0-7EAA-45e1-8E7D-64414AFF281A}   File Prop Sheet Page Helper
{E96F5460-09CE-4f46-88B1-F4B6B4A8E252}   Windows Media Player Transcode Files Cache
Cleanup Handler
{E974D26D-3D9B-4D47-88CC-3872F2DC3585}   XPS Object Factory
{E9A6AB1B-0C9C-44AC-966E-560C2771D1E8}   DrawAttrsXP Class
{E9F4EBAB-D97B-463e-A2B1-C54EE3F9414D}   Net Scheme Handler
{EA022610-0748-4c24-B229-6C507EBDFDBB}   CLSID_HomeGroupCtrlServer
{EA2C6B24-C590-457B-BAC8-4A0F9B13B5B8}   User Account Control Settings
{EA30C654-C62C-441f-AC00-95F9A196782C}   GestureRecognizer Class
{EA502722-A23D-11D1-A7D3-0000F87571E3}   Group Policy Object
{EA678830-235D-11d2-A8B6-0000F8084F96}   CLSID_IPropPatchRequest
{ea72d00e-4960-42fa-ba92-7792a7944c1d}   Run as different user context menu handler
{EA7BAE70-FB3B-11CD-A903-00AA00510EA3}
{EA7BAE71-FB3B-11CD-A903-00AA00510EA3}
{ea8b451c-5a19-49cf-bc5e-98accca49ef3}   Library Factory
{EA9155A3-8A39-40b4-8963-D3C761B18371}   PerfTrack TaskHandler class
{ea9a0595-056e-4d74-980f-bb53f6bb9f8d}   PSFactoryBuffer
{EAC8A024-21E2-4523-AD73-A71A0AA2F56A}   WbemQuery
{eb124705-128b-40d4-8dd8-d93ed12589a4}   WPL property store
{eb4d075a-65c0-476b-956c-c605eade03f7}   DemuxRender
{EB56EAE8-BA51-11d2-B121-00805FC73204}
{EB6B4457-F013-4E5A-9B05-1D44E4D6FAEB}   HomeGroup Sharing Hosted Listener
{EB87E1BD-3233-11D2-AEC9-00C04FB68820}   WbemStatusCode
{EBB08C45-6C4A-4FDC-AE53-4EB8C4C7DB8E}   TF_LangBarMgr
{EC00BA63-C73A-4679-AC8D-69366C766989}   SBE Stats - receiver side
{EC529B00-1A1F-11D1-BAD9-00609744111A}   WDM Streaming VPE VBI Property Set
Interface Handler
{ecabafaa-7f19-11d2-978e-0000f8757e2a}   Activity Property Unmarshal Class
{ecabafab-7f19-11d2-978e-0000f8757e2a}   SecurityEnvoy
{ecabafac-7f19-11d2-978e-0000f8757e2a}   Transaction Property Unmarshal Class
{ecabafad-7f19-11d2-978e-0000f8757e2a}   NonRootTransactionEnvoy
{ecabafae-7f19-11d2-978e-0000f8757e2a}   sca Class
{ecabafaf-7f19-11d2-978e-0000f8757e2a}   ClassFactory Activator Class
{ecabafb0-7f19-11d2-978e-0000f8757e2a}   obja Class
{ecabafb1-7f19-11d2-978e-0000f8757e2a}   stapa Class
{ecabafb2-7f19-11d2-978e-0000f8757e2a}   vca Class
{ecabafb3-7f19-11d2-978e-0000f8757e2a}   User Context Object
{ecabafb4-7f19-11d2-978e-0000f8757e2a}   User Context Properties Association Object
{ecabafb5-7f19-11d2-978e-0000f8757e2a}   PoolMgr Class
{ecabafb6-7f19-11d2-978e-0000f8757e2a}   Object Pool Activator Class
{ecabafb7-7f19-11d2-978e-0000f8757e2a}   Contruction Activator Class
{ecabafb9-7f19-11d2-978e-0000f8757e2a}   COM+ Instance Tracking Component
{ecabafbc-7f19-11d2-978e-0000f8757e2a}   COM+ Event Notification Server
{ecabafc0-7f19-11d2-978e-0000f8757e2a}   cfw Class
{ecabafc2-7f19-11d2-978e-0000f8757e2a}   Queued Components Recorder
```

Page 97

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {ecabafc3-7f19-11d2-978e-0000f8757e2a} | QC Listener Class |
| {ecabafc4-7f19-11d2-978e-0000f8757e2a} | Queued Components Player |
| {ecabafc6-7f19-11d2-978e-0000f8757e2a} | New Moniker |
| {ecabafc7-7f19-11d2-978e-0000f8757e2a} | Queue Moniker |
| {ecabafc9-7f19-11d2-978e-0000f8757e2a} | QC Queue Administration Class |
| {ecabafca-7f19-11d2-978e-0000f8757e2a} | COM+ QC Dead Letter Queue Listener Starter |
| {ecabafcb-7f19-11d2-978e-0000f8757e2a} | QC Marshal Interceptor Class |
| {ecabafcc-7f19-11d2-978e-0000f8757e2a} | Partition Property Unmarshal Class |
| {ecabafcd-7f19-11d2-978e-0000f8757e2a} | Tracking Info Collection Unmarshal Class |
| {ecabafce-7f19-11d2-978e-0000f8757e2a} | Tracking Info Object Unmarshal Class |
| {ecabafcf-7f19-11d2-978e-0000f8757e2a} | EventRegistrar Class |
| {ecabafd0-7f19-11d2-978e-0000f8757e2a} | Soap Activator Class |
| {ecabafd3-7f19-11d2-978e-0000f8757e2a} | ObjWrapperMarshaler Class |
| {ecabb0a8-7f19-11d2-978e-0000f8757e2a} | COM+ Services GetSecurityCallContext |
| {ecabb0aa-7f19-11d2-978e-0000f8757e2a} | Byot Server Extended Object |
| {ecabb0ab-7f19-11d2-978e-0000f8757e2a} | MTSEvents Class |
| {ecabb0ac-7f19-11d2-978e-0000f8757e2a} | MTSLocator Class |
| {ecabb0bd-7f19-11d2-978e-0000f8757e2a} | CrmClerk Class |
| {ecabb0be-7f19-11d2-978e-0000f8757e2a} | CrmRecoveryClerk Class |
| {ecabb0bf-7f19-11d2-978e-0000f8757e2a} | MessageMover Class |
| {ecabb0c0-7f19-11d2-978e-0000f8757e2a} | DispenserManager |
| {ECABB0C3-7F19-11D2-978E-0000F8757E2A} | ComEvents.ComServiceEvents |
| {ecabb0c4-7f19-11d2-978e-0000f8757e2a} | Debug Dump Server |
| {ecabb0c5-7f19-11d2-978e-0000f8757e2a} | Partition Moniker |
| {ECABB0C6-7F19-11D2-978E-0000F8757E2A} | ComEvents.ComSystemAppEventData |
| {ecabb0c7-7f19-11d2-978e-0000f8757e2a} | SOAP Moniker |
| {ecabb0c8-7f19-11d2-978e-0000f8757e2a} | CServiceConfig Class |
| {ECABB0C9-7F19-11D2-978E-0000F8757E2A} | |
| {ECABB0CA-7F19-11D2-978E-0000F8757E2A} | |
| {ECD32AEA-746F-4dcb-BF68-082757FAFF18} | DynamicRenderer Class |
| {ECD4FC4D-521C-11D0-B792-00A0C90312E1} | Shell Rebar BandSite |
| {ECD4FC4E-521C-11D0-B792-00A0C90312E1} | Shell Band Site Menu |
| {ECD4FC4F-521C-11D0-B792-00A0C90312E1} | Menu Desk Bar |
| {ECE71064-011D-45b7-AEF2-3B626985E937} | CPropertyObject Class |
| {ECF03A32-103D-11d2-854D-006008059367} | MyDocs Drop Target |
| {ecf5bf46-e3b6-449a-b56b-43f58f867814} | Identity Store Profile Notification |
| {ed1d0fdf-4414-470a-a56d-cfb68623fc58} | Play with Windows Media Player |
| {ED228FDF-9EA8-4870-83b1-96b02CFE0D52} | Games Explorer |
| {ed50fc29-b964-48a9-afb3-15ebb9b97f36} | printhood delegate folder |
| {ed6ae9cf-ad35-46b7-ac30-3f8b9eb5349f} | TryHarderFactory |
| {ED7BA470-8E54-465E-825C-99712043E01C} | All Tasks |
| {ED81C073-1F84-4ca8-A161-183C776BC651} | Lat/Long Report Class |
| {ED8C108E-4349-11D2-91A4-00C04F7969E8} | XML HTTP Request |
| {ED999FF5-223A-4052-8ECE-0B10C8DBAA39} | ActualWbemUnauthenticatedLocator Class |
| {edb5f444-cb8d-445a-a523-ec5ab6ea33c7} | Share Manager |
| {EDD36029-D753-4862-AA5B-5BCCAD2A4D29} | Property Store Collection |
| {edd749de-2ef1-4a80-98d1-81f20e6df58e} | PLAP Logon Provider Filter |
| {EDF6970E-4557-4BC5-86C2-C7E52A06B27F} | PSFactoryBuffer |
| {EE09B103-97E0-11CF-978F-00A02463E06F} | Scripting.Dictionary |
| {ee2e9ce0-0fe1-4eea-8f30-e4728b56f183} | Category Drop Target |
| {EE366069-1832-420F-B381-0479AD066F19} | |
| {EE4DA6A4-8C52-4a63-BBB8-97C93D7E1B6C} | APPLICATION__X_MS_WMD Moniker Class |
| {EE8E4870-A889-4DC4-969F-F38F707F4AC2} | CTaskCondition |
| {eea0c191-dda8-4656-8fc4-72bdedba8a78} | Library Property Store |
| {EEBEACC0-D281-4557-A0F4-B2193F86B1EA} | Net Connect Page Class |
| {EEC5DCCA-05DC-4B46-8AF7-2881C1635AEA} | System.ServiceModel.Internal.TransactionBridge |
| {EEC6993A-B3FD-11D2-A916-00C04FB98638} | Microsoft USB PID Class Driver |
| {eec97550-47a9-11cf-b952-00aa0051fe20} | HTML File persistent handler |
| {EF011F79-4000-406D-87AF-BFFB3FC39D57} | DirectSoundCompressorDMO |
| {EF114C90-CD1D-484E-96E5-09CFAF912A21} | DirectSoundDistortionDMO |
| {ef1c0450-0b48-4384-94ae-d1cb35641f86} | Categorizer Factory |
| {EF3E932C-D40B-4F51-8CCF-3F98F1B29D5D} | DirectSoundEchoDMO |

Page 98

```
                        SOFTWARE OUTPUT.txt
{ef43ecfe-2ab9-4632-bf21-58909dd177f0}  Folder Customization Tab
{EF4D1E1A-1C87-4AA8-8934-E68E4367468D}  WebCheck
{ef5db4c2-9312-422c-9152-411cd9c4dd84}  PortableDeviceService Class
{EF8AD2D1-AE36-11D1-B2D2-006097DF8C11}  Global Folder Settings
{EF985E71-D5C7-42D4-BA4D-2D073E2E96F4}  DirectSoundI3DL2ReverbDMO
{EFA24E64-B078-11D0-89E4-00C04FC9E26E}
{EFB4A0CB-A01F-451C-B6B7-56F02F77D76F}  GenericRecognizer Class
{EFCA3D92-DFD8-4672-A603-7420894BAD98}  DirectSoundFlangerDMO
{EFE3FA02-45D7-4920-BE96-53FA7F35B0E6}  BDA Tuning Model DVB Terrestrial 2 Locator
{EFE6629C-81F7-4281-BD91-C9D604A95AF6}  DirectSoundChorusDMO
{F020E586-5264-11d1-A532-0000F8757D7E}
{F0285374-DFF1-11D3-B433-00C04F8ECD78}  ConsolePower Class
{F0291081-E87C-4E07-97DA-A0A03761E586}  Drawing
{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}  Computers and Devices
{F04CC277-03A2-4277-96A9-77967471BDFF}  Sync Center Conflict Properties Extension
{f07f3920-7b8c-11cf-9be8-00aa004b9986}  Microsoft Office Filter
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}  Background Intelligent Transfer Control
Class 1.5
{F08C5AC2-E722-4116-ADB7-CE41B527994B}  Bluetooth Authentication Agent SSO
{f0ae1542-f497-484b-a175-a20db09144ba}
{F1390A9A-A3F4-4E5D-9C5F-98F3BD8D935C}  Sync Setup Delegate Folder
{F198A89A-5042-4294-ADF1-CB163E549798}  Win32_EncryptableVolumeProvider Class
{F1E752C3-FD72-11D0-AEF6-00C04FB6DD2C}  DocConfig 1.0 Object
{f1f3b524-b27f-4a64-8d26-c654800b79d3}  Run Backup AutoPlay Handler Class
{F20487CC-FC04-4B1E-863F-D9801796130B}  Sync Center Shell Service Object
(Internal)
{F2102C37-90C3-450C-B3F6-92BE1693BDF2}  Windows Security Center ISV API
{F22F5E05-585C-4def-8523-6555CFBC0CB3}  CTocEntry
{f235ce7d-b143-4d4f-ad93-64e48d53a5fb}  CLSID_KnownAutoListManager
{F2472B49-5214-4D3A-A662-04F09250D694}  WlanDlgNonUIFinishPage Class
{f26a669a-bcbb-4e37-abf9-7325da15f931}  AutoPlayVerb
{f270c64a-ffb8-4ae4-85fe-3a75e5347966}  ADs Security Utility Object
{f2c3faae-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.OU
{F31091EA-B0A8-11D6-B6FC-005056C00008}  CmiFactory Class
{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}  Microsoft WBEM New Event Subsystem
{F3364BA0-65B9-11CE-A9BA-00AA004AE837}  Shell File System Folder
{F3368374-CF19-11d0-B93D-00A0C90312e1}  OrderListExport
{f371728a-6052-4d47-827c-d039335dfe0a}  Mpeg4 Decoder DMO
{F37AFD4F-E736-4980-8650-A486B1F2DF25}  Windows_Search_OutlookToolbar
{F37C5810-4D3F-11d0-B4BF-00AA00BBB723}  Security Shell Extension
{F382DA49-9148-4a22-AF78-C378DFC32D02}  MS_InstalledGameProv Class
{F3BDFAD3-F276-49e9-9B17-C474F48F0764}  CQueryWinSAT Class
{F3C633A2-46C8-498E-8FBB-CC6F721BBCDE}
{f3cc4ca3-22c2-40ec-ac3c-89d8a43373b0}  Include the selected folder in a library.
{f3d06e7c-1e45-4a26-847e-f9fcdee59be0}  Copy as Path Menu
{f4086d4e-2e05-428b-92de-87d8d0bb4262}  Pnrp Helper Class
{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}  JScript Language
{f414c261-6ac0-11cf-b6d1-00aa00bbbb58}  JScript Language Authoring
{f414c262-6ac0-11cf-b6d1-00aa00bbbb58}  JScript Language Encoding
{f447b69e-1884-4a7e-8055-346f74d6edb3}  Resampler DMO
{F46316E4-FB1B-46eb-AEDF-9520BFBB916A}  Dynamic Storage Object
{F4655419-DAF2-42ab-9178-3B6AC903170C}  RNWF MSM Helper Class
{f4be747e-45c4-4701-90f1-d49d9ac30248}  PerfCenter Enabler
{F5078F19-C551-11D3-89B9-0000F81FE221}  XML Parser
{F5078F27-C551-11D3-89B9-0000F81FE221}
{F5078F31-C551-11D3-89B9-0000F81FE221}  XML Parser 3.0
{F5078F32-C551-11D3-89B9-0000F81FE221}  XML DOM Document 3.0
{F5078F33-C551-11D3-89B9-0000F81FE221}  Free Threaded XML DOM Document 3.0
{F5078F34-C551-11D3-89B9-0000F81FE221}  XML Schema Cache 3.0
{F5078F35-C551-11D3-89B9-0000F81FE221}  XML HTTP 3.0
{F5078F36-C551-11D3-89B9-0000F81FE221}  XSL Template 3.0
{F5078F37-C551-11D3-89B9-0000F81FE221}
{F5078F39-C551-11D3-89B9-0000F81FE221}  XML Data Source Object 3.0
                        Page 99
```

```
                         SOFTWARE OUTPUT.txt
    {F5078F3F-C551-11D3-89B9-0000F81FE221}  XML Moniker 3.0
    {F5078F40-C551-11D3-89B9-0000F81FE221}  XML Document 3.0
    {F5078F41-C551-11D3-89B9-0000F81FE221}  XML Island 3.0
    {f507f854-308b-401e-a1b7-b55ba6ba679a}  Association Property Handler
    {F562A2C8-E850-4F05-8E7A-E7192E4E6C23}  PSFactoryBuffer
    {F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}  Action Center Shell Service Object
    {F5A55D36-8750-432C-AB52-AD49A016EABC}  Microsoft WMI Provider Subsystem Binding
Factory
    {F5B63656-069D-4E80-B4FD-9E0DB16604D8}
    {f5d121ed-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.User
    {f5d121ee-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Group
    {f5d121ef-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Domain
    {f5d121f0-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Contact
    {f5d121f3-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Volume
    {f5d121f4-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Computer
    {F5D3E63B-CB0F-4628-A478-6D8244BE36B1}
    {F5F75737-2843-4F22-933D-C76A97CDA62F}  Microsoft WMI Provider Subsystem Decoupled
Basic Event Provider
    {f60163ce-2b8d-458d-ab2c-40f215767514}  CLSID_IndexScopeFiller
    {F6166DAD-D3BE-4ebd-8419-9B5EAD8D0EC7}  ShellItemArray Shell Namespace helper
    {F618C514-DFB8-11D1-A2CF-00805FC79235}  Catalog2 Class
    {F61FFEC1-754F-11d0-80CA-00AA005B4383}  BandProxy
    {F62D062C-4732-44D2-BD62-124B8AE1657C}  WMPlayer PluginsPropPage Class
    {F6B96EDA-1A94-4476-A85F-4D3DC7B39C3F}  DvbSiParser Class
    {F6BEC032-233E-4B58-BEE9-DE13942BF136}  PSFactoryBuffer
    {F6D90F11-9C73-11D3-B32E-00C04F990BB4}  XML DOM Document
    {F6D90F12-9C73-11D3-B32E-00C04F990BB4}  Free Threaded XML DOM Document
    {F6D90F14-9C73-11D3-B32E-00C04F990BB4}  XML Data Source Object
    {F6D90F16-9C73-11D3-B32E-00C04F990BB4}  XML HTTP
    {f713df56-e581-482c-9453-3e934eac5899}
    {F72A76A0-EB0A-11D0-ACE4-0000C0CC16BA}  KsDataTypeHandlerVideo2
    {F72A76E0-EB0A-11D0-ACE4-0000C0CC16BA}  KsDataTypeHandlerVBI
    {f744e496-1b5a-489e-81dc-fbd7ac6298a8}  Microsoft PenInputPanel Control
    {f77d9c1c-5aff-4341-b028-57f7510aa91c}  CLSID_AssociationListExtender
    {f792beee-aeaf-4ebb-ab14-8bc5c8c695a8}  Media Foundation MP2demux
    {F7A4F1DA-96C3-4BCF-BEB3-1D9FFDE89EE9}  ComCacheCleanup 1.0 Object
    {F7AFD75B-BF8C-4a11-BDB9-04AD66182F84}  MF Video Presenter 2
    {F7B9271E-46D8-4B6A-B5CF-E6A4F7F49732}  Alternates Class
    {f7c0039a-4762-488a-b4b3-760ef9a1ba9b}  PortableDeviceFTM Class
    {f7ffe0a0-a4f5-44b5-949e-15ed2bc66f9d}  MSScreen 9 encoder DMO
    {F80608CB-5A88-4046-9E4B-3C1BB368F2DA}  WMPDMCPlaylist Class
    {f81b1b56-7613-4ee4-bc05-1fab5de5c07e}  MF MPEG-4 Property Handler
    {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6}  Shell extensions for sharing
    {F82DF8F7-8B9F-442E-A48C-818EA735FF9B}  Pen and Touch Control Panel
    {F8383852-FCD3-11d1-A6B9-006097DF5BD4}  Progress Dialog
    {F8388A40-D5BB-11D0-BE5A-0080C706568E}  Infinite Pin Tee Filter
    {f83cbf45-1c37-4ca1-a78a-28bcb91642ec}  CD Audio Burning Hook
    {f85d5d94-6851-44f7-bb3a-bfd0949abf1d}  Tree property value cache
    {F885120E-3789-4fd9-865E-DC9B4A6412D2}  IARPUninstallStringLauncher
    {f8a56d3e-e304-4a9f-a916-5187019d7759}
    {f8b8412b-dea3-4130-b36c-5e8be73106ac}  CLSID_PreviewHtml
    {F8D253D9-89A4-4daa-87B6-1168369F0B21}  UpdateServiceManager Class
    {F8FB6E07-55E6-4BB9-96BC-2393A039CEE7}  UIGlobalNotify Class
    {F90B5F36-367B-402A-9DD1-BC0FD59D8F62}
    {F90FE5FE-E88B-4578-9C81-79210FD53D41}  Infrastructure Adapter Page Selection
Class
    {F91D96C7-8509-4D0B-AB26-A0DD10904BB7}  CMpeg2Stream
    {F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}  Windows Script Host Shell Object
    {F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}  Windows Script Host Network Object
    {F9769A06-7ACA-4E39-9CFB-97BB35F0E77E}  BDA Tuning Model Auxiliary Inputs Tuning
Space
    {F979439C-48B7-4525-AB0E-EEE06439227A}  Windows Media Player
WMEncPrivatePluginConnector Class
                              Page 100
```

SOFTWARE OUTPUT.txt

```
{F97B8A60-31AD-11CF-B2DE-00DD01101B85}  Stretch
{F9A7AB61-C0BC-490e-A7FE-BFF26B327A3F}  OpenSearch Result Context Menu
{F9AE8980-7E52-11d0-8964-00C04FD611D7}  MSIDXS
{F9AE8981-7E52-11d0-8964-00C04FD611D7}  MSIDXS ErrorLookup
{f9bcb2f0-7df0-4a39-932e-bdef29dfb16b}  Authentication UI Session Control
{F9F4D292-87F5-4E2D-98A1-590391932490}  Windows Media Player WMEncBasicEdit Class
{FA10746C-9B63-4b6c-BC49-FC300EA5F256}  Enhanced Video Renderer
{FA4B375A-45B4-4D45-8440-263957B11623}  Microsoft DVBS Network Provider
{FA5FE7C5-6A1D-4B11-B41F-F959D6C76500}  Microsoft MPEG-2 Media Foundation Media
Sink
{FA7C375B-66A7-4280-879D-FD459C84BB02}  WebDVD Adminitration class
{FA8A68B2-C864-4BA2-AD53-D3876A87494B}  StreamBufferConfig
{FAB24754-0440-439b-A223-B1D360062D1D}  Dhcp Quarantine Enforcement Client
Callback Component
{FABD6EA5-AE10-4E7A-B83B-5F07ACC84214}  WPD Settings Review Page Class
{FAE3D380-FEA4-4623-8C75-C6B61110B681}
{FAF53CC4-BD73-4E36-83F1-2B23F46E513E}  VssEvent
{FB012959-F4F6-44D7-9D09-DAA087A9DB57}
{FB40360C-547E-4956-A3B9-D4418859BA66}
{fb479c02-9ec4-4fed-8599-debe037452cb}  Shell Hardware Mixed Content Handler
Cancelled
{FB4CDF30-A741-421d-BCFA-6CC530D053FB}  Microsoft.SQLLITE.MOBILE.OLEDB.3.0
{FB64825E-498C-45E8-ADD4-37E0C4FC68A6}  SBE Stats - Mpeg2 Video Stream Analysis
{FB74F625-7D25-4455-B840-7B870B5B9322}  Windows Media SDK MSB Source Plugin
{fbe5c2f7-027e-4033-afcd-faa04af9be8d}  Authentication UI Background Dialog
{fbeb8a05-beee-4442-804e-409d6c4515e9}  ShellFolder for CD Burning
{fbebb71b-a592-4880-b096-9429ebe119db}  Extensible L2Sec Helper Class
{fc1ee10b-7ef6-41b5-bb60-98d26dd9fcd1}
{FC220AD8-A72A-4EE8-926E-0B7AD152A020}  MXXMLWriter
{FC5B8A24-DB05-4A01-8388-22EDF6C2BBBA}  Bidi Spooler APIs
{FC772AB0-0C7F-11D3-8FF2-00A0C9224CF4}  BDA MPEG2 Transport Information Filter
{fcc2867c-69ea-4d85-8058-7c214e611c97}  Authentication UI Terminal Services Bump
Dialog Server
{FCC74B77-EC3E-4dd8-A80B-008A702075A9}  ARP UninstallString Launcher
{fccf70c8-f4d7-4d8b-8c17-cd6715e37fff}  Search Control
{FCF7A6F2-3300-4386-9A4F-0DD4E3226507}  WmiPerf Instance Provider
{FD0A5AF3-B41D-11D2-9C95-00C04F7971E0}  IBDA_DeviceControl
{FD351EA1-4173-4AF4-821D-80D4AE979048}  Stream Buffer V2 Source
{FD853CD9-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeInternational
{FD853CDB-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeBody
{FD853CDC-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessageParts
{FD853CDD-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeAllocator
{FD853CDE-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeSecurity
{FD853CDF-7F86-11d0-8252-00C04FD85AB4}  CLSID_IVirtualStream
{FD853CE0-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeHeaderTable
{FD853CE1-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimePropertySet
{FD853CE2-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessageTree
{FD853CE3-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessage
{FD853CE6-7F86-11d0-8252-00C04FD85AB4}  CLSID_ISMTPTransport
{FD853CE7-7F86-11d0-8252-00C04FD85AB4}  CLSID_IPOP3Transport
{FD853CE8-7F86-11d0-8252-00C04FD85AB4}  CLSID_INNTPTransport
{FD853CE9-7F86-11d0-8252-00C04FD85AB4}  CLSID_IRASTransport
{FD853CEA-7F86-11d0-8252-00C04FD85AB4}  CLSID_IRangeList
{FD853CEB-7F86-11d0-8252-00C04FD85AB4}  CLSID_IIMAPTransport
{FD853CED-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimePropertySchema
{FDD384CC-78C6-4E6D-8694-1DACBEE57F96}  PSFactoryBuffer
{fe1290f0-cfbd-11cf-a330-00aa00c16e65}  @%SystemRoot%\system32\dsquery.dll,-553
{FE12CD81-5158-4bd8-A37C-A621BC0E143B}
{fe5afcf2-e681-4ada-9703-ef39b8ecb9bf}  Library Description
{fe7c0d2b-27f1-4e97-951b-cf6e165eeab6}  TSMFActivate Class
{FEA4300C-7959-4147-B26A-2377B9E7A91D}  DirectSoundFullDuplex Object
{FEB50740-7BEF-11CE-9BD9-0000E202599C}  MPEG Video Codec
{FEC52D45-D657-42c3-B43E-BF64B95E7072}  WIA Preview Component
```

Page 101

ø

SOFTWARE OUTPUT.txt
```
{fecd606e-7161-4cbc-a868-4703867823ea}  WMDM Transcode Property Page
{FEF10FA2-355E-4e06-9381-9B24D7F7CC88}
{FF036D13-5D4B-46DD-B10F-106693D9FE4F}
{FF151822-B0BF-11D1-A80D-000000000000}  Microsoft OLE DB Root Binder for Internet
Publishing
{FF2A742B-CA25-4507-BD93-6BA9B8E8965F}  Fat MSM Helper Class
{ff363bfe-4941-4179-a81c-f3f1ca72d820}  HomeGroup SSO
{ff48dba4-60ef-4201-aa87-54103eef594e}  UIAutomation Client Central Class
{ff8a32e3-a9a7-4093-b9c4-5b5b4f30ab63}  CLSID_ResultShape
{ff9e6131-a8c1-4188-aa03-82e9f10a05a8}  Elevatable Shortcut
{FFB8655F-81B9-4fce-B89C-9A6BA76D13E7}  Shell Execute Hardware Event Handler
{FFCDB781-D71C-4D10-BD5F-0492EAFFD90A}  PSFactoryBuffer
{ffe1df5f-9f06-46d3-af27-f1fc10d63892}  HomeGroup CPL Advanced Settings Writer
{FFE2A43C-56B9-4bf5-9A79-CC6D4285608A}  Windows Photo Viewer Image Verbs
```
-------------------------------------------
cmd_shell v.20130405
(Software) Gets shell open cmds for various file types

Classes\exefile\shell\open\command
LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)
  Cmd: "%1" %*

Classes\cmdfile\shell\open\command
LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)
  Cmd: "%1" %*

Classes\batfile\shell\open\command
LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)
  Cmd: "%1" %*

Classes\csfile\shell\open\command not found.

Classes\htafile\shell\open\command
LastWrite Time Tue Dec 29 18:43:07 2015 (UTC)
  Cmd: C:\Windows\SysWOW64\mshta.exe "%1" %*

Classes\piffile\shell\open\command
LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)
  Cmd: "%1" %*


Clients\StartMenuInternet\IExplore.exe\shell\open\command
LastWrite Time Mon Apr 18 15:50:45 2016 (UTC)
  Cmd: C:\Program Files\Internet Explorer\iexplore.exe
-------------------------------------------
codeid v.20100608
(Software) Gets CodeIdentifier DefaultLevel value

CodeID
Policies\Microsoft\Windows\Safer\CodeIdentifiers
  LastWrite time: Tue Jul 14 04:49:20 2009 Z


-------------------------------------------
ctrlpnl v.20100116
(Software) Get Control Panel info from Software hive


Microsoft\Windows\CurrentVersion\Control Panel

Cpls key
SMSCFGRC    C:\WINDOWS\CCM\SMSCFGRC.cpl

don't load key

Page 102

SOFTWARE OUTPUT.txt

```
hdwwiz.cpl
telephon.cpl
appwiz.cpl
ncpa.cpl
sysdm.cpl
desk.cpl
inetcpl.cpl
joy.cpl
mmsys.cpl
Firewall.cpl
powercfg.cpl
intl.cpl
timedate.cpl
main.cpl
collab.cpl
irprops.cpl
tabletpc.cpl
infocardcpl.cpl
bthprops.cpl
```

System.ControlPanel.Category [Tue Jul 14 04:53:25 2009 UTC]
Category -1,4
   %SystemRoot%\System32\Speech\SpeechUX\sapi.cpl

{305CA226-D286-468e-B848-2B2E8E697B74} 2 [Mon Apr 18 15:31:08 2016 UTC]
Category 0x0,0x1,0x2,0x5
   %SystemRoot%\system32\nvCpl.cpl

Sounds, Speech, and Audio Devices
   %SystemRoot%\System32\RTDSnM64.cpl

Performance and Maintenance
   C:\WINDOWS\CCM\SMSCFGRC.cpl


----------------------------------------
defbrowser v.20091116
(Software) Gets default browser setting from HKLM

Default Browser Check #1
Clients\StartMenuInternet
LastWrite Time Tue Apr 19 20:41:00 2016 (UTC)

Default Browser : IEXPLORE.EXE

Default Browser Check #2
Classes\HTTP\shell\open\command
LastWrite Time Tue Apr 19 20:03:56 2016 (UTC)

Default Browser = "C:\Program Files\Internet Explorer\IEXPLORE.EXE" %1
----------------------------------------
Launching direct v.20120513
Microsoft

Wow6432Node\Microsoft
Mon Apr 18 15:26:54 2016    Direct3D\MostRecentApplication - iexplore.exe
Mon Apr 18 15:26:54 2016    DirectDraw\MostRecentApplication - iexplore.exe

----------------------------------------
disablesr v.20120914
(Software) Gets the value that turns System Restore either on or off

Microsoft\Windows NT\CurrentVersion\SystemRestore
                              Page 103

```
                              SOFTWARE OUTPUT.txt
LastWrite Time Wed Apr 20 15:39:52 2016 (UTC)

DisableSR value not found.
--------------------------------------------
drivers32 v.20130408
(Software) Get values from the Drivers32 key

Microsoft\Windows NT\CurrentVersion\Drivers32
LastWrite Time Mon Apr 18 15:28:56 2016 (UTC)
  VIDC.YVYU - msyuv.dll
  aux1 - wdmaud.drv
  aux - wdmaud.drv
  vidc.i420 - iyuv_32.dll
  msacm.imaadpcm - imaadp32.acm
  MSVideo8 - VfWWDM32.dll
  midi - wdmaud.drv
  msacm.msadpcm - msadp32.acm
  wavemapper - msacm32.drv
  VIDC.UYVY - msyuv.dll
  midimapper - midimap.dll
  vidc.msvc - msvidc32.dll
  mixer1 - wdmaud.drv
  vidc.mrle - msrle32.dll
  VIDC.YUY2 - msyuv.dll
  VIDC.YVU9 - tsbyuv.dll
  mixer - wdmaud.drv
  msacm.l3acm - C:\Windows\System32\l3codeca.acm
  VIDC.IYUV - iyuv_32.dll
  wave - wdmaud.drv
  msacm.msgsm610 - msgsm32.acm
  msacm.msg711 - msg711.acm
  wave1 - wdmaud.drv
  midi1 - wdmaud.drv

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
LastWrite Time Mon Apr 18 15:28:12 2016 (UTC)
  vidc.uyvy - msyuv.dll
  vidc.iyuv - iyuv_32.dll
  aux1 - wdmaud.drv
  aux - wdmaud.drv
  vidc.cvid - iccvid.dll
  vidc.i420 - iyuv_32.dll
  msacm.imaadpcm - imaadp32.acm
  vidc.yvu9 - tsbyuv.dll
  midi - wdmaud.drv
  msacm.msadpcm - msadp32.acm
  wavemapper - msacm32.drv
  midimapper - midimap.dll
  vidc.yvyu - msyuv.dll
  vidc.msvc - msvidc32.dll
  mixer1 - wdmaud.drv
  vidc.mrle - msrle32.dll
  mixer - wdmaud.drv
  vidc.yuy2 - msyuv.dll
  msacm.l3acm - C:\Windows\SysWOW64\l3codeca.acm
  msacm.msgsm610 - msgsm32.acm
  wave - wdmaud.drv
  msacm.msg711 - msg711.acm
  wave1 - wdmaud.drv
  midi1 - wdmaud.drv

--------------------------------------------
drwatson v.20081219
```

                                   Page 104

SOFTWARE OUTPUT.txt
(Software) Gets Dr. Watson settings from Software hive

Microsoft\Windows NT\CurrentVersion\AeDebug
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
Debugging is Disabled

Microsoft\DrWatson not found.

Analysis Tips: For Dr. Watson settings information check:
http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/RegistryTips/Registry
Tools/DrWatson.html
--------------------------------------------
emdmgmt v.20120207
(Software) Gets contents of EMDMgmt subkeys and values

EMDMgmt
Microsoft\Windows NT\CurrentVersion\EMDMgmt
LastWrite Time Tue Apr 19 20:03:50 2016 (UTC)

HD-PSU2
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    VSN: 44FA34

FDA
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    VSN: B6C2-DCA0

Disk&Ven_&Prod_&Rev_2.20
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: 0718011120035AF&0
    VSN: 6085-4400

Disk&Ven_&Prod_&Rev_2.20
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: 0718011120035AF&0
    VSN: 20C7-421F

Disk&Ven_&Prod_&Rev_8.07
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: B57D6A2F&0
    Vol Name: Configuration Manager 2012
    VSN: 1A3B-F68E

Disk&Ven_&Prod_&Rev_PMAP
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: 07032B5A180AA664&0
    Vol Name: THUMBDRIVE
    VSN: B650-E7C9

Disk&Ven_&Prod_&Rev_PMAP
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: 070B43D2DE271C28&0
    Vol Name: USB DISK
    VSN: 12DA-241C

Disk&Ven_&Prod_&Rev_PMAP
    LastWrite: Tue Apr 19 20:03:50 2016 Z
    SN: 070B43D2DE271C28&0
    Vol Name: USB DISK
    VSN: FEB5-787A

Disk&Ven_&Prod_&Rev_PMAP
    LastWrite: Tue Apr 19 20:03:50 2016 Z
                                     Page 105

SOFTWARE OUTPUT.txt
```
   SN: 070B43D2DE271C28&0
   Vol Name: USB DISK
   VSN: 1E35-B51B

Disk&Ven_hp&Prod_USB_FLASH_DRIVE&Rev_1.00
   LastWrite: Tue Apr 19 20:03:50 2016 Z
   SN: 002354D46B97AC5102CF01C0&0
   Vol Name: ITUNES
   VSN: 2CC2-CDDB
   LastTestedTime: Mon Mar 21 11:10:22 2016 Z

Disk&Ven_PNY&Prod_USB_2.0_FD&Rev_1100
   LastWrite: Tue Apr 19 20:03:50 2016 Z
   SN: ACB3HD1000000240&0
   Vol Name: WORKFILES
   VSN: 8A30-CC6A

Disk&Ven_SanDisk&Prod_Cruzer&Rev_1.20
   LastWrite: Tue Apr 19 20:03:50 2016 Z
   SN: 200544568018E7B0762E&0
   VSN: 2099-41D8
   LastTestedTime: Tue Apr 19 18:52:27 2016 Z


------------------------------------------
ie_version v.20140717
(Software) Get IE version and build

Microsoft\Internet Explorer
LastWrite Time Wed Apr 20 15:39:52 2016 (UTC)


IE Build    = 99600
IE Version = 9.11.9600.18163
svcUpdateVersion (IE 10/11) = 11.0.27
svcVersion (IE 10/11)       = 11.0.9600.18163
------------------------------------------
imagefile v.20131007
(Software) Checks IFEO subkeys for Debugger & CWDIllegalInDllSearch values

Microsoft\Windows NT\CurrentVersion\Image File Execution Options
No Debugger/CWDIllegalInDllSearch values found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options not
found.
------------------------------------------
init_dlls v.20110309
(Software) Check for odd **pInit_Dlls keys

init_dlls
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite: Mon Apr 18 15:30:11 2016

LoadAppInit_DLLs
------------------------------------------
installedcomp v.20130911
(Software) Get info about Installed Components and StubPath values

Microsoft\Active Setup\Installed Components
LastWrite Time Wed Apr 20 15:39:52 2016 (UTC)

Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18163
```
Page 106

SOFTWARE OUTPUT.txt

Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -EnableTLS
Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18163
Mon Apr 18 15:51:11 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -UserConfig
Mon Apr 18 15:50:45 2016 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -DisableSSL3
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Wed Dec 30 12:50:33 2015
(UTC),{2D46B6DC-2207-486B-B523-A557E6D54B47},ClearIconCache, v.11,0,9600,16428,
C:\windows\system32\cmd.exe /D /C start C:\windows\system32\ie4uinit.exe
-ClearIconCache
Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,7601,18840
Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI
Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll
Tue Dec 29 18:43:08 2015
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install
Tue Dec 29 18:23:34 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,
v.4,0,30319,0
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.6,1,7601,17514
Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,
v.2,0,50727,0
Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
%SystemRoot%\system32\themeui.dll
Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,
v.4,71,1113,0
Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0

Wow6432Node\Microsoft\Active Setup\Installed Components
LastWrite Time Tue Apr 19 20:41:00 2016 (UTC)

Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18163

Page 107

SOFTWARE OUTPUT.txt
Wed Apr 20 15:39:52 2016 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -EnableTLS
Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18163
Tue Apr 19 20:41:00 2016 (UTC),{8A69D345-D564-463c-AFF1-A69D9E530F96}, v.43,0,0,0,
"C:\Program Files
(x86)\Google\Chrome\Application\50.0.2661.75\Installer\chrmstp.exe"
--configure-user-settings --verbose-logging --system-level --multi-install --chrome
Mon Apr 18 15:54:27 2016 (UTC),{08B0E5C0-4FCB-11CF-AAA5-00401C608500},JAVAVM,
v.5,0,5000,0
Mon Apr 18 15:51:12 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},
Mon Apr 18 15:51:11 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -UserConfig
Mon Apr 18 15:50:45 2016 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -DisableSSL3
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Wed Dec 30 12:50:33 2015
(UTC),{2D46B6DC-2207-486B-B523-A557E6D54B47},ClearIconCache, v.11,0,9600,16428,
C:\windows\system32\cmd.exe /D /C start C:\windows\system32\ie4uinit.exe
-ClearIconCache
Wed Dec 30 12:48:40 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,7601,18840
Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI
Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll
Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,7601,18840
Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI
Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll
Wed Dec 30 07:06:36 2015 (UTC),{0EEB34F6-991D-4a1b-8EEB-772DA0EADB22},Microsoft Lync
2010, v.4.0.7577.4486
Tue Dec 29 18:43:08 2015
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install
Tue Dec 29 18:43:08 2015

Page 108

SOFTWARE OUTPUT.txt

. (UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install
Tue Dec 29 18:23:34 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,
v.4,0,30319,0
Tue Dec 29 18:23:33 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,
v.4,0,30319,0
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.6,1,7601,17514
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.6,1,7601,17514, "%ProgramFiles(x86)%\Windows Mail\WinMail.exe"
OCInstallUserConfigOE
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.6,1,7601,17514
Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,
v.2,0,50727,0
Tue Jul 14 04:49:55 2009 (UTC),{7C028AF8-F614-47B3-82DA-BA94E41B1089},.NETFramework,
v.2,0,50727,0
Tue Jul 14 04:49:04 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
%SystemRoot%\system32\themeui.dll
Tue Jul 14 04:49:04 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEX,
v.4,71,1113,0
Tue Jul 14 04:49:04 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Tue Jul 14 04:49:04 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0
Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
%SystemRoot%\system32\themeui.dll
Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEX,
v.4,71,1113,0
Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0
--------------------------------------------
Launching installer v.20120917
(Software) Determines product install information

Installer
Microsoft\Windows\CurrentVersion\Installer\UserData

User SID: S-1-5-18
Key       : 0000410911000000000000000F01FEC
LastWrite: Tue Dec 29 15:55:19 2015
20160420 - Microsoft Office Professional Plus 2010 14.0.7015.1000 (Microsoft
Corporation)

Key       : 000041091A0090400000000000F01FEC
LastWrite: Tue Dec 29 15:51:44 2015
20151230 - Microsoft Office OneNote MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key       : 0000410944009040000000000F01FEC
LastWrite: Tue Dec 29 15:51:47 2015
20151229 - Microsoft Office InfoPath MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key       : 0000410951009040000000000F01FEC

Page 109

SOFTWARE OUTPUT.txt
LastWrite: Tue Dec 29 15:51:50 2015
20151229 - Microsoft Office Access MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 0000410951109040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:14 2015
20151229 - Microsoft Office Shared Setup Metadata MUI (English) 2010 14.0.7015.1000
(Microsoft Corporation)

Key      : 0000410961009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:20 2015
20151230 - Microsoft Office Excel MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 0000410961109040010000000000F01FEC
LastWrite: Tue Dec 29 15:51:32 2015
20151229 - Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010
14.0.7015.1000 (Microsoft Corporation)

Key      : 0000410971109040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:53 2015
20151229 - Microsoft Office Access Setup Metadata MUI (English) 2010 14.0.7015.1000
(Microsoft Corporation)

Key      : 0000410981009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:17 2015
20151230 - Microsoft Office PowerPoint MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 0000410991009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:56 2015
20151229 - Microsoft Office Publisher MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109A1009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:27 2015
20151230 - Microsoft Office Outlook MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109A2000000010000000000F01FEC
LastWrite: Tue Dec 29 15:52:25 2015
20151230 - Microsoft Office Office 64-bit Components 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109A2009040010000000000F01FEC
LastWrite: Tue Dec 29 15:51:30 2015
20151229 - Microsoft Office Shared 64-bit MUI (English) 2010 14.0.7015.1000
(Microsoft Corporation)

Key      : 00004109AB009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:23 2015
20151229 - Microsoft Office Groove MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109B1009040000000000000F01FEC
LastWrite: Tue Dec 29 15:52:00 2015
20151230 - Microsoft Office Word MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109C2009040000000000000F01FEC
LastWrite: Tue Dec 29 15:51:41 2015
20151229 - Microsoft Office Proofing (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Page 110

SOFTWARE OUTPUT.txt

Key      : 00004109E60090400000000000F01FEC
LastWrite: Tue Dec 29 15:51:11 2015
20151230 - Microsoft office Shared MUI (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109F10090400000000000F01FEC
LastWrite: Tue Dec 29 15:51:39 2015
20151230 - Microsoft office Proof (English) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109F100A0C00000000000F01FEC
LastWrite: Tue Dec 29 15:51:34 2015
20151230 - Microsoft office Proof (Spanish) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 00004109F100C0400000000000F01FEC
LastWrite: Tue Dec 29 15:51:37 2015
20151230 - Microsoft office Proof (French) 2010 14.0.7015.1000 (Microsoft
Corporation)

Key      : 003FDA6004B887B42B1D28C91E00089B
LastWrite: Tue Apr 19 20:41:24 2016
20160419 - Cisco Jabber 10.5.0.37889 (Cisco Systems, Inc)

Key      : 07233B137D427034482F3A8268638BA3
LastWrite: Mon Apr 18 15:57:46 2016
20160418 - Check Point Endpoint Security - Full Disk Encryption 7.5.100.25 (Check
Point Software Technologies Ltd)

Key      : 0DFF11082E0C1394989B074CA9FFDCE6
LastWrite: Mon Apr 18 15:56:15 2016
20160418 - WebEx Productivity Tools 2.36.13053.10004 (Cisco WebEx LLC)

Key      : 1007C6B46D7C017319E3B52CF3EC196E
LastWrite: Tue Dec 29 16:06:55 2015
20151229 - Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148
9.0.30729.4148 (Microsoft Corporation)

Key      : 1279CD7A68949714BB983A9E595485C4
LastWrite: Wed Apr 20 14:56:02 2016
20160420 - Adobe Flash Player 21 NPAPI 21.0.0.182 (Adobe Systems Incorporated)

Key      : 166F59DC4C5A5F446AAACEDD192C04BD
LastWrite: Mon Apr 18 15:45:54 2016
20160418 - WinZip 17.5 17.5.10480 (WinZip Computing, S.L. )

Key      : 1926E8D15D0BCE53481466615F760A7F
LastWrite: Tue Dec 29 22:29:24 2015
20160418 - Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219 10.0.40219
(Microsoft Corporation)

Key      : 1A4908760526B674A9FF34674EF831C5
LastWrite: Wed Dec 30 12:23:40 2015
20151230 - Citrix online plug-in (DV) 12.1.0.30 (Citrix Systems, Inc.)

Key      : 1af2a8da7e60d0b429d7e6453b3d0182
LastWrite: Mon Apr 18 16:00:06 2016
20160418 - Microsoft Visual C++ 2005 Redistributable (x64) 8.0.61000 (Microsoft
Corporation)

Key      : 1D5E3C0FEDA1E123187686FED06E995A
LastWrite: Tue Dec 29 22:29:19 2015

Page 111

SOFTWARE OUTPUT.txt

20160418 - Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219 10.0.40219
(Microsoft Corporation)

Key       : 1F61ECF34CCC81A47A7B8873CF4CBA1B
LastWrite: Wed Dec 30 12:20:19 2015
20151230 - eRoom 7 Client 503.196 (eRoom)

Key       : 2187CE6B546CDCD4CB1BC4D70F826883
LastWrite: Mon Apr 18 15:54:40 2016
20160418 - WebEx Poll Questionnaire Editor 29.13.30.10011 (Cisco WebEx LLC)

Key       : 21EE4A31AE32173319EEFE3BD6FDFFE3
LastWrite: Mon Apr 18 15:30:35 2016
20160418 - Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 12.0.21005
(Microsoft Corporation)

Key       : 22BEFC8F7E2A1793E9ADB411DEFE1C58
LastWrite: Mon Apr 18 15:30:36 2016
20160418 - Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 12.0.21005
(Microsoft Corporation)

Key       : 2572AF4636286C342B286BDC45FC141A
LastWrite: Wed Dec 30 12:24:52 2015
20151230 - EMC SourceOne Offline Access 6.72.0017 (EMC Corporation)

Key       : 2FD49CAE087C459429F4E03E87A0571D
LastWrite: Tue Apr 19 20:40:20 2016
20160419 - Cisco IP Communicator 8.6.3.0 (Cisco Systems, Inc.)

Key       : 300C9B2DDC3A0A44D95E25EF89C6305E
LastWrite: Mon Apr 18 16:02:28 2016
20160418 - McAfee Host Intrusion Prevention 8.00.0600 (McAfee, Inc.)

Key       : 305B553211B9944468D1C171842B3602
LastWrite: Mon Apr 18 15:28:10 2016
20160418 - Realtek Audio COM Components 1.0.2 (Realtek Semiconductor Corp.)

Key       : 37954E682535F9341A51E2E84E4D1004
LastWrite: Wed Dec 30 12:22:12 2015
20160418 - ActivClient x64 6.2 (ActivIdentity)

Key       : 4BEA594979BAED93C82408E6FE57CE7A
LastWrite: Wed Dec 30 13:27:50 2015
20151229 - Microsoft Visual Studio 2010 Tools for Office Runtime (x64) 10.0.50908
(Microsoft Corporation)

Key       : 4EA42A62D9304AC4784BF238120671FF
LastWrite: Mon Apr 18 15:54:07 2016
20160418 - Java(TM) 6 Update 17 6.0.170 (Sun Microsystems, Inc.)

Key       : 4EA42A62D9304AC4784BF2381206830F
LastWrite: Mon Apr 18 15:54:25 2016
20160418 - Java(TM) 6 Update 38 6.0.380 (Oracle)

Key       : 51A61408B41252F40A52DEE67865132F
LastWrite: Mon Apr 18 15:56:54 2016
20160418 - Cisco AnyConnect Secure Mobility Client 3.1.05160 (Cisco Systems, Inc.)

Key       : 51BB133E91DB2E8419E6E79453F709F5
LastWrite: Wed Apr 20 13:20:08 2016
20160420 - McAfee Agent 5.00.2011 (McAfee, Inc.)

Key       : 53F51841BE20BE248B1429B8ACD20D74
                              Page 112

SOFTWARE OUTPUT.txt

LastWrite: Mon Apr 18 15:54:43 2016
20160418 - Network Recording Player 29.13.40.10011 (Cisco WebEx LLC)

Key        : 5B8447711A1E2454D913B0D2B66D7CE3
LastWrite: Wed Apr 20 13:00:14 2016
20160420 - WebEx Training Manager for Firefox or Chrome 29.13.40.10011 (Cisco WebEx LLC)

Key        : 5DBCA9191C3E07D4E8C24CB7D3593BA0
LastWrite: Mon Apr 18 15:37:38 2016
20160418 - DisplayLink Core Software 7.9.630.0 (DisplayLink Corp.)

Key        : 62DBF9290209B993A9A757D1160F9B24
LastWrite: Mon Apr 18 15:30:36 2016
20160418 - Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 12.0.21005 (Microsoft Corporation)

Key        : 67D6ECF5CD5FBA732B8B22BAC8DE1B4D
LastWrite: Tue Dec 29 18:26:52 2015
20151229 - Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 9.0.30729.6161 (Microsoft Corporation)

Key        : 68AB67CA3301000077060000000000050
LastWrite: Mon Apr 18 15:44:21 2016
20160418 - Adobe Acrobat X Pro 10.1.16 (Adobe Systems)

Key        : 68AB67CA40803301919500814261761515
LastWrite: Mon Apr 18 16:27:08 2016
20160418 - Adobe Refresh Manager 1.8.0 (Adobe Systems Incorporated)

Key        : 69F04C30238C91242AA0141FC925C84A
LastWrite: Mon Apr 18 15:54:47 2016
20160418 - WebEx Document Suite 29.13.40.10011 (Cisco WebEx LLC)

Key        : 6B1D51EC6B91D4D4F834FCD5C23365FF
LastWrite: Mon Apr 18 15:58:41 2016
20160418 - McAfee VirusScan Enterprise 8.8.04001 (McAfee, Inc.)

Key        : 6D02C9913D0101243B16740602F965EA
LastWrite: Wed Dec 30 12:23:31 2015
20151230 - Citrix online plug-in (Web) 12.1.0.30 (Citrix Systems, Inc.)

Key        : 6E815EB96CCE9A53884E7857C57002F0
LastWrite: Tue Dec 29 18:27:34 2015
20151229 - Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 9.0.30729.6161 (Microsoft Corporation)

Key        : 6E8D947A316B3EB3F8F540C548BE2AB9
LastWrite: Mon Apr 18 15:30:36 2016
20160418 - Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 12.0.21005 (Microsoft Corporation)

Key        : 6EFF1ED8BCFF36942A8F3DBFFCF28188
LastWrite: Mon Apr 18 15:54:44 2016
20160418 - WebEx Training Manager for Internet Explorer 29.13.40.10011 (Cisco WebEx LLC)

Key        : 703563AF369161D4DB4411C3F830A7DA
LastWrite: Wed Dec 30 12:23:41 2015
20151230 - Citrix online plug-in (HDX) 12.1.0.30 (Citrix Systems, Inc.)

Key        : 7054D343F7993554F968B28BF1910AE5
LastWrite: Mon Apr 18 15:31:09 2016

Page 113

SOFTWARE OUTPUT.txt
20160419 - Configuration Manager Client 5.00.8239.1000 (Microsoft Corporation)

Key      : 71B0EB18B3654D541B8975126E6C56DC
LastWrite: Tue Dec 29 16:07:33 2015
20151230 - Microsoft Lync 2010 4.0.7577.4486 (Microsoft Corporation)

Key      : 7BC0F7E72988BE83FB04A0A683006403
LastWrite: Wed Apr 20 12:59:26 2016
20160420 - Google Chrome 66.56.118 (Google, Inc.)

Key      : 7CBFA89A7A5D1A647859AEEBF2557A6D
LastWrite: Tue Dec 29 16:08:46 2015
20151229 - Microsoft Office Live Meeting 2007 8.0.6362.91 (Microsoft Corporation)

Key      : 836DD5B2D473DC64A9B8EA414EFE3A15
LastWrite: Wed Apr 20 12:59:59 2016
20160420 - Cisco WebEx Meeting Center for Firefox or Chrome 29.13.41.10011 (Cisco WebEx LLC)

Key      : 87143C29976B38C4CA33E7CF6E3DE610
LastWrite: Wed Apr 20 14:56:14 2016
20160420 - Adobe Flash Player 21 ActiveX 21.0.0.182 (Adobe Systems Incorporated)

Key      : 875BCCE3E405A7F48A4BFCF4B339B944
LastWrite: Wed Dec 30 12:23:38 2015
20151230 - Citrix online plug-in (USB) 12.1.0.30 (Citrix Systems, Inc.)

Key      : 8B592D0980ABE7849B40E02624904A01
LastWrite: Mon Apr 18 15:30:46 2016
20160418 - Microsoft Policy Platform 1.2.3602.0 (Microsoft Corporation)

Key      : 8BC556559E3C0274F999553596930FED
LastWrite: Mon Apr 18 15:54:39 2016
20160418 - WebEx Event Manager for Internet Explorer 29.13.41.10011 (Cisco WebEx LLC)

Key      : A089CE062ADB6BC44A720BA745894BAC
LastWrite: Tue Apr 19 20:52:00 2016
20160419 - Google Update Helper 1.3.29.5 (Google Inc.)

Key      : A91CBC048F06F654FA921C293499AFA0
LastWrite: Mon Apr 18 15:37:43 2016
20160418 - DisplayLink Graphics 7.9.665.0 (DisplayLink Corp.)

Key      : c1c4f01781cc94c4c8fb1542c0981a2a
LastWrite: Mon Apr 18 16:00:02 2016
20151230 - Microsoft Visual C++ 2005 Redistributable 8.0.61001 (Microsoft Corporation)

Key      : C28643E881181F13CBC489DC69571E2C
LastWrite: Mon Apr 18 15:43:30 2016
20160420 - Microsoft .NET Framework 4 Extended 4.0.30319 (Microsoft Corporation)

Key      : CB8F1D5EA3CCDD942AC2D9BF37A8B6C0
LastWrite: Mon Apr 18 15:54:42 2016
20160418 - Cisco WebEx Meeting Center for Internet Explorer 29.13.41.10011 (Cisco WebEx LLC)

Key      : CF041C82706219944B7C40FC9366C5F2
LastWrite: Tue Apr 19 20:55:59 2016
20160419 - GlobalSubmit Review 2014 8.2.2 (GlobalSubmit, Inc.)

Key      : CF83C93EC343D3D4D8AC86C1F78F15A8
Page 114

SOFTWARE OUTPUT.txt
LastWrite: Mon Apr 18 15:54:19 2016
20160418 - SAFE Servlet 7.05.00.219 (Guidance Software)

Key       : CFD2C1F142D260E3CB8B271543DA9F98
LastWrite: Tue Dec 29 16:05:49 2015
20151229 - Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
9.0.30729.4148 (Microsoft Corporation)

Key       : D2E6C29A5434ABB46AC78AB2868E6164
LastWrite: Mon Apr 18 15:54:46 2016
20160418 - WebEx Support Manager for Internet Explorer 29.13.40.10011 (Cisco WebEx
LLC)

Key       : D7314F9862C648A4DB8BE2A5B47BE100
LastWrite: Wed Dec 30 07:04:36 2015
20160420 - Microsoft Silverlight 5.1.41212.0 (Microsoft Corporation)

Key       : DCBA27FA0816E114F9DB744513738CAC
LastWrite: Mon Apr 18 15:56:55 2016
20160418 - Cisco AnyConnect Start Before Login Module 3.1.05160 (Cisco Systems,
Inc.)

Key       : DFC90B5F2B0FFA63D84FD16F6BF37C4B
LastWrite: Mon Apr 18 15:42:19 2016
20160420 - Microsoft .NET Framework 4 Client Profile 4.0.30319 (Microsoft
Corporation)

Key       : EECA7043EEEC3F64DBABFF81034D4CD2
LastWrite: Wed Dec 30 12:23:18 2015
20151230 - Access Card Utility 1.4.2 (Deloitte LLP)

Key       : F40DC675E77504848AFEC9A86724DA66
LastWrite: Mon Apr 18 15:56:54 2016
20160418 - Cisco AnyConnect Diagnostics and Reporting Tool 3.1.05160 (Cisco Systems,
Inc.)

Key       : FB60CDF5D3D37634F8BFF4FABC1679D2
LastWrite: Mon Apr 18 15:57:15 2016
20160418 - Cisco Systems VPN Client 5.0.07.0440 5.0.7 (Cisco Systems, Inc.)

Key       : FFA086E2F47FBEC4CB34300AC62CE86A
LastWrite: Wed Apr 20 12:59:43 2016
20160420 - WebEx Event Manager for Firefox or Chrome 29.13.41.10011 (Cisco WebEx
LLC)

User SID: S-1-5-21-2431487851-277683799-2983902431-500
----------------------------------------
kb950582 v.20081212
(Software) KB950582 - Gets autorun settings from HKLM hive

NoDriveTypeAutoRun    0xff
HonorAutorunSetting not found.

Autorun settings in the HKLM hive take precedence over those in
the HKCU hive.
----------------------------------------
LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not found.
Wow6432Node\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not
found.
LANDesk\Inventory\LogonHistory\Logons not found.
Wow6432Node\LANDesk\Inventory\LogonHistory\Logons not found.
----------------------------------------
macaddr v.20090118

Page 115

SOFTWARE OUTPUT.txt

(Software) --

Microsoft\Windows Genuine Advantage not found.
-------------------------------------------
mrt v.20080804
(Software) Check to see if Malicious Software Removal Tool has been run

Key Path: Microsoft\RemovalTools\MRT
LastWrite Time Mon Apr 18 15:29:01 2016 (UTC)

Error getting Version information: Can't call method "get_data" on an undefined
value at C:\Users\mdickson\Desktop\Tools\rrv2.8/plugins\mrt.pl line 55.

-------------------------------------------
msis v.20090911
(Software) Determine MSI packages installed on the system


Classes\Installer\Products
LastWrite Time Wed Apr 20 14:56:14 2016 (UTC)

Wed Apr 20 15:01:53 2016 (UTC)
   Microsoft Office Professional Plus 2010;C:\MSOCache\All
Users\{90140000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi
Wed Apr 20 14:59:18 2016 (UTC)
   Microsoft Silverlight;c:\7b77a2156d89ac7db8abc3d7\silverlight.msi
Wed Apr 20 14:56:14 2016 (UTC)
   Adobe Flash Player 21 ActiveX;install_flash_player_21_active_x.msi
Wed Apr 20 14:56:02 2016 (UTC)
   Adobe Flash Player 21 NPAPI;install_flash_player_21_plugin.msi
Wed Apr 20 13:37:20 2016 (UTC)
   Microsoft .NET Framework 4 Extended;C:\WINDOWS\TEMP\Microsoft .NET Framework 4
Setup_4.0.30319\netfx_Extended_x64.msi
Wed Apr 20 13:36:48 2016 (UTC)
   Microsoft .NET Framework 4 Client Profile;C:\WINDOWS\TEMP\Microsoft .NET Framework
4 Setup_4.0.30319\netfx_Core_x64.msi
Wed Apr 20 13:20:08 2016 (UTC)
   McAfee Agent;MFEagent_x64.msi
Wed Apr 20 13:00:14 2016 (UTC)
   WebEx Training Manager for Firefox or
Chrome;C:\WINDOWS\ccmcache\3\Training_Center\attcns_firefox.msi
Wed Apr 20 12:59:59 2016 (UTC)
   Cisco WebEx Meeting Center for Firefox or
Chrome;C:\WINDOWS\ccmcache\3\Mtg_Center\atmcns_firefox.msi
Wed Apr 20 12:59:43 2016 (UTC)
   WebEx Event Manager for Firefox or
Chrome;C:\WINDOWS\ccmcache\3\Event_Center\atecns_firefox.msi
Wed Apr 20 12:59:26 2016 (UTC)
   Google Chrome;googlechromestandaloneenterprise.msi
Tue Apr 19 20:55:59 2016 (UTC)
   GlobalSubmit Review 2014;Review.msi
Tue Apr 19 20:52:00 2016 (UTC)
   Google Update Helper;C:\Program Files
(x86)\Google\Update\1.3.29.5\GoogleUpdateHelper.msi
Tue Apr 19 20:41:24 2016 (UTC)
   Cisco Jabber;CiscoJabberSetup.msi
Tue Apr 19 20:40:20 2016 (UTC)
   Cisco IP Communicator;CiscoIPCommunicatorSetup.msi
Tue Apr 19 20:00:03 2016 (UTC)
   Configuration Manager
Client;C:\WINDOWS\ccmsetup\{72875A95-4007-4DAC-88D8-66366F9A5045}\client.msi
Mon Apr 18 16:27:08 2016 (UTC)
   Adobe Refresh Manager;C:\Program Files (x86)\Common
Page 116

SOFTWARE OUTPUT.txt
Files\Adobe\ARM\1.0\Cache\Arm_001824166751_8417287593495712044028555111 3286767.msi
Mon Apr 18 16:02:28 2016 (UTC)
   McAfee Host Intrusion
Prevention;C:\_SMSTaskSequence\Packages\PS1002F3\McAfeeHIP_ClientSetup_X64.msi
Mon Apr 18 16:00:10 2016 (UTC)
   Microsoft Visual C++ 2010  x64 Redistributable -
10.0.40219;C:\3cb5f26f2fc5f9d5c4e783d5be\vc_red.msi
Mon Apr 18 16:00:05 2016 (UTC)
   Microsoft Visual C++ 2010  x86 Redistributable -
10.0.40219;C:\dac6f6cbcef6992dde8507\vc_red.msi
Mon Apr 18 15:58:41 2016 (UTC)
   McAfee VirusScan Enterprise;VSE880.MSI
Mon Apr 18 15:57:46 2016 (UTC)
   Check Point Endpoint Security - Full Disk Encryption;Pointsec for PC.msi
Mon Apr 18 15:57:15 2016 (UTC)
   Cisco Systems VPN Client
5.0.07.0440;C:\_SMSTaskSequence\Packages\FDA00080\5.0.07.0440\vpnclient_setup.msi
Mon Apr 18 15:56:55 2016 (UTC)
   Cisco AnyConnect Start Before Login
Module;C:\_SMSTaskSequence\Packages\FDA002D5\anyconnect-gina-win-3.1.05160-pre-deplo
y-k9.msi
Mon Apr 18 15:56:54 2016 (UTC)
   Cisco AnyConnect Secure Mobility
Client;C:\_SMSTaskSequence\Packages\FDA002D5\anyconnect-win-3.1.05160-pre-deploy-k9.
msi
   Cisco AnyConnect Diagnostics and Reporting
Tool;C:\_SMSTaskSequence\Packages\FDA002D5\anyconnect-dart-win-3.1.05160-k9.msi
Mon Apr 18 15:54:53 2016 (UTC)
   WebEx Productivity
Tools;C:\_SMSTaskSequence\Packages\PS1002D1\Productivity_Tools\ptools.msi
Mon Apr 18 15:54:47 2016 (UTC)
   WebEx Document
Suite;C:\_SMSTaskSequence\Packages\PS1002D1\Productivity_Tools\atucfsuite.msi
Mon Apr 18 15:54:46 2016 (UTC)
   WebEx Support Manager for Internet
Explorer;C:\_SMSTaskSequence\Packages\PS1002D1\Support_Center\SC_Win.msi
Mon Apr 18 15:54:44 2016 (UTC)
   WebEx Training Manager for Internet
Explorer;C:\_SMSTaskSequence\Packages\PS1002D1\Training_Center\attcie_ie.msi
Mon Apr 18 15:54:43 2016 (UTC)
   Network Recording
Player;C:\_SMSTaskSequence\Packages\PS1002D1\Players\ARF_nbr2player.msi
Mon Apr 18 15:54:42 2016 (UTC)
   Cisco WebEx Meeting Center for Internet
Explorer;C:\_SMSTaskSequence\Packages\PS1002D1\Mtg_Center\atmcie_ie.msi
Mon Apr 18 15:54:40 2016 (UTC)
   WebEx Poll Questionnaire
Editor;C:\_SMSTaskSequence\Packages\PS1002D1\Event_Center\polleditor.msi
Mon Apr 18 15:54:39 2016 (UTC)
   WebEx Event Manager for Internet
Explorer;C:\_SMSTaskSequence\Packages\PS1002D1\Event_Center\atecie_ie.msi
Mon Apr 18 15:54:25 2016 (UTC)
   Java(TM) 6 Update
38;C:\WINDOWS\SysWOW64\config\systemprofile\AppData\LocalLow\Sun\Java\jre1.6.0_38\jr
e1.6.0_38.msi
Mon Apr 18 15:54:19 2016 (UTC)
   SAFE Servlet;C:\_SMSTaskSequence\Packages\PS10004B\Encase\Setup.msi
Mon Apr 18 15:54:07 2016 (UTC)
   Java(TM) 6 Update 17;C:\_SMSTaskSequence\Packages\FDA0004E\jre1.6.0_17.msi
Mon Apr 18 15:45:54 2016 (UTC)
   WinZip 17.5;C:\_SMSTaskSequence\Packages\FDA0022E\winzip175-64.msi
Mon Apr 18 15:45:32 2016 (UTC)
   ActivClient x64;Z:\Applications\ActivClient(6.2.0.179)\ActivClient x64 6.2.msi
Page 117

SOFTWARE OUTPUT.txt

Mon Apr 18 15:44:52 2016 (UTC)
    Adobe Acrobat X Pro;C:\_SMSTaskSequence\Packages\FDA000C7\Adobe Acrobat X\AcroPro.msi
Mon Apr 18 15:37:43 2016 (UTC)
    DisplayLink Graphics;C:\_SMSTaskSequence\Packages\PS1002C3\Setup.msi
Mon Apr 18 15:37:38 2016 (UTC)
    DisplayLink Core
Software;C:\_SMSTaskSequence\Packages\PS1002C3\DisplayLinkCore.msi
Mon Apr 18 15:30:46 2016 (UTC)
    Microsoft Policy Platform;C:\WINDOWS\ccmsetup\MicrosoftPolicyPlatformSetup.msi
Mon Apr 18 15:30:43 2016 (UTC)
    Microsoft Visual C++ 2005 Redistributable
(x64);C:\WINDOWS\TEMP\IXP000.TMP\vcredist.msi
Mon Apr 18 15:30:36 2016 (UTC)
    Microsoft Visual C++ 2013 x86 Additional Runtime -
12.0.21005;C:\ProgramData\Package
Cache\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}v12.0.21005\packages\vcRuntimeAdditional
_x86\vc_runtimeAdditional_x86.msi
    Microsoft Visual C++ 2013 x64 Additional Runtime -
12.0.21005;C:\ProgramData\Package
Cache\{929FBD26-9020-399B-9A7A-751D61F0B942}v12.0.21005\packages\vcRuntimeAdditional
_amd64\vc_runtimeAdditional_x64.msi
    Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005;C:\ProgramData\Package
Cache\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}v12.0.21005\packages\vcRuntimeMinimum_am
d64\vc_runtimeMinimum_x64.msi
Mon Apr 18 15:30:35 2016 (UTC)
    Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005;C:\ProgramData\Package
Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x8
6\vc_runtimeMinimum_x86.msi
Mon Apr 18 15:28:10 2016 (UTC)
    Realtek Audio COM Components;C:\Program Files\Realtek\Audio\HDA\SetupRAPCOM.msi
Wed Dec 30 12:33:34 2015 (UTC)
    Microsoft Visual C++ 2005 Redistributable;C:\WINDOWS\TEMP\IXP000.TMP\vcredist.msi
Wed Dec 30 12:24:53 2015 (UTC)
    EMC SourceOne Offline Access;C:\windows\Downloaded
Installations\{8E968E35-FC28-4D31-98CB-E6152C341C97}\ES1_OfflineAccess.msi
Wed Dec 30 12:23:41 2015 (UTC)
    Citrix online plug-in
(HDX);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\
Extract\CitrixHDXMediaStreamForFlash-ClientInstall.msi
Wed Dec 30 12:23:40 2015 (UTC)
    Citrix online plug-in
(DV);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\E
xtract\DesktopViewer.msi
Wed Dec 30 12:23:38 2015 (UTC)
    Citrix online plug-in
(USB);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\
Extract\GenericUSB.msi
Wed Dec 30 12:23:31 2015 (UTC)
    Citrix online plug-in
(Web);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\
Extract\ICAWebWrapper.msi
Wed Dec 30 12:23:18 2015 (UTC)
    Access Card Utility;Z:\Applications\Access Card Utility
1.4.2\AccessCardUtilitySetup.msi
Wed Dec 30 12:20:19 2015 (UTC)
    eRoom 7
Client;C:\Users\ADMINI~1\AppData\Local\Temp\{CD8C4F5A-FA28-4C9C-B8E0-8FDCAC57609D}\e
Room7Client.msi
Wed Dec 30 10:06:56 2015 (UTC)
    Microsoft Office Proof (English) 2010;C:\MSOCache\All
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.msi
Wed Dec 30 09:57:51 2015 (UTC)

Page 118

SOFTWARE OUTPUT.txt
    Microsoft Office OneNote MUI (English) 2010;C:\MSOCache\All
Users\{90140000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.msi
Wed Dec 30 09:57:46 2015 (UTC)
    Microsoft Office Office 64-bit Components 2010;C:\MSOCache\All
Users\{90140000-0011-0000-0000-0000000FF1CE}-C\office64ww.msi
Wed Dec 30 09:55:56 2015 (UTC)
    Microsoft Office Word MUI (English) 2010;C:\MSOCache\All
Users\{90140000-001B-0409-0000-0000000FF1CE}-C\WordMUI.msi
Wed Dec 30 09:55:53 2015 (UTC)
    Microsoft Office Outlook MUI (English) 2010;C:\MSOCache\All
Users\{90140000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.msi
Wed Dec 30 09:55:13 2015 (UTC)
    Microsoft Office Shared MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0115-0409-0000-0000000FF1CE}-C\officeMUI.msi
Wed Dec 30 08:44:57 2015 (UTC)
    Microsoft Office PowerPoint MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi
Wed Dec 30 08:44:54 2015 (UTC)
    Microsoft Office Excel MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi
Wed Dec 30 08:42:54 2015 (UTC)
    Microsoft Office Proof (Spanish) 2010;C:\MSOCache\All
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.msi
Wed Dec 30 08:42:51 2015 (UTC)
    Microsoft Office Proof (French) 2010;C:\MSOCache\All
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.msi
Wed Dec 30 07:06:36 2015 (UTC)
    Microsoft Lync 2010;C:\Program Files (x86)\OCSetup\Lync.msi
Wed Dec 30 00:26:49 2015 (UTC)
    Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0116-0409-1000-0000000FF1CE}-C\office64MUISet.msi
Wed Dec 30 00:26:47 2015 (UTC)
    Microsoft Office Shared 64-bit MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0116-0409-1000-0000000FF1CE}-C\office64MUI.msi
Wed Dec 30 00:26:28 2015 (UTC)
    Microsoft Office Publisher MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi
Wed Dec 30 00:26:25 2015 (UTC)
    Microsoft Office Proofing (English) 2010;C:\MSOCache\All
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proofing.msi
Wed Dec 30 00:26:12 2015 (UTC)
    Microsoft Office Shared Setup Metadata MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0115-0409-0000-0000000FF1CE}-C\officeMUISet.msi
Wed Dec 30 00:26:06 2015 (UTC)
    Microsoft Office InfoPath MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi
Wed Dec 30 00:26:02 2015 (UTC)
    Microsoft Office Groove MUI (English) 2010;C:\MSOCache\All
Users\{90140000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.msi
Wed Dec 30 00:25:55 2015 (UTC)
    Microsoft Office Access Setup Metadata MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.msi
Wed Dec 30 00:25:52 2015 (UTC)
    Microsoft Office Access MUI (English) 2010;C:\MSOCache\All
Users\{90140000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.msi
Tue Dec 29 22:29:49 2015 (UTC)
    Microsoft Visual Studio 2010 Tools for Office Runtime
(x64);c:\ffc0de99483c3b8404d06720ece77548\vstor40_x64.msi
Tue Dec 29 18:27:34 2015 (UTC)
    Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.6161;c:\7bfee4305bf8ac2d04340f06\vc_red.msi
Tue Dec 29 18:26:52 2015 (UTC)
    Microsoft Visual C++ 2008 Redistributable - x64
                        Page 119

SOFTWARE OUTPUT.txt
9.0.30729.6161;c:\f0f7a84a229330edc7\vc_red.msi
Tue Dec 29 16:08:46 2015 (UTC)
  Microsoft Office Live Meeting 2007;Z:\Applications\Microsoft Office Live Meeting
2007\LMConsole.msi
Tue Dec 29 16:06:55 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x64
9.0.30729.4148;c:\d6a21fa13028cb2bd6c663889fb6be\vc_red.msi
Tue Dec 29 16:05:49 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.4148;c:\01cb7e3f01e8447dcd8b\vc_red.msi
-----------------------------------
networkcards v.20080325
(Software) Get NetworkCards

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Intel(R) Ethernet Connection (3) I218-LM   [Mon Apr 18 15:27:40 2016]
Intel(R) Dual Band Wireless-AC 7265   [Mon Apr 18 15:28:04 2016]
-----------------------------------
Launching networklist v.20141204
(Software) Collects network info from Vista+ NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
fda.gov
  Key LastWrite      : Wed Apr 20 16:36:26 2016 UTC
  DateLastConnected: Wed Apr 20 12:36:26 2016
  DateCreated       : Mon Apr 18 11:27:49 2016
  DefaultGatewayMac: 00-1D-45-AC-DF-BF
  Type              : wired
  Category          : Domain

Network
  Key LastWrite      : Mon Apr 18 15:30:04 2016 UTC
  DateLastConnected: Mon Apr 18 11:30:04 2016
  DateCreated       : Mon Apr 18 11:30:04 2016
  DefaultGatewayMac: 00-1D-45-AC-DF-BF
  Type              : wired
  Category          : Public

-----------------------------------
networkuid v.20100312
(Software) Gets Network key UID value

Microsoft\Windows NT\CurrentVersion\Network not found.
-----------------------------------
product v.20100325
(Software) Get installed product info


Microsoft\Windows\CurrentVersion\Installer\UserData

S-1-5-18
Wed Apr 20 15:01:53 2016 Z
  Microsoft Office Professional Plus 2010 v.14.0.7015.1000, 20160420
Wed Apr 20 14:59:18 2016 Z
  Microsoft Silverlight v.5.1.41212.0, 20160420
Wed Apr 20 14:56:14 2016 Z
  Adobe Flash Player 21 ActiveX v.21.0.0.182, 20160420
Wed Apr 20 14:56:02 2016 Z
  Adobe Flash Player 21 NPAPI v.21.0.0.182, 20160420
Wed Apr 20 13:37:19 2016 Z
  Microsoft .NET Framework 4 Extended v.4.0.30319, 20160420
                              Page 120

SOFTWARE OUTPUT.txt
Wed Apr 20 13:36:47 2016 Z
   Microsoft .NET Framework 4 Client Profile v.4.0.30319, 20160420
Wed Apr 20 13:20:08 2016 Z
   McAfee Agent v.5.00.2011, 20160420
Wed Apr 20 13:00:14 2016 Z
   WebEx Training Manager for Firefox or Chrome v.29.13.40.10011, 20160420
Wed Apr 20 12:59:59 2016 Z
   Cisco WebEx Meeting Center for Firefox or Chrome v.29.13.41.10011, 20160420
Wed Apr 20 12:59:43 2016 Z
   WebEx Event Manager for Firefox or Chrome v.29.13.41.10011, 20160420
Wed Apr 20 12:59:26 2016 Z
   Google Chrome v.66.56.118, 20160420
Tue Apr 19 20:55:59 2016 Z
   GlobalSubmit Review 2014 v.8.2.2, 20160419
Tue Apr 19 20:52:00 2016 Z
   Google Update Helper v.1.3.29.5, 20160419
Tue Apr 19 20:41:20 2016 Z
   Cisco Jabber v.10.5.0.37889, 20160419
Tue Apr 19 20:40:20 2016 Z
   Cisco IP Communicator v.8.6.3.0, 20160419
Tue Apr 19 20:00:03 2016 Z
   Configuration Manager Client v.5.00.8239.1000, 20160419
Mon Apr 18 16:27:08 2016 Z
   Adobe Refresh Manager v.1.8.0, 20160418
Mon Apr 18 16:02:28 2016 Z
   McAfee Host Intrusion Prevention v.8.00.0600, 20160418
Mon Apr 18 16:00:10 2016 Z
   Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219 v.10.0.40219, 20160418
Mon Apr 18 16:00:06 2016 Z
   Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000, 20160418
Mon Apr 18 16:00:05 2016 Z
   Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219 v.10.0.40219, 20160418
Mon Apr 18 16:00:02 2016 Z
   Microsoft Visual C++ 2005 Redistributable v.8.0.61001, 20151230
Mon Apr 18 15:58:41 2016 Z
   McAfee VirusScan Enterprise v.8.8.04001, 20160418
Mon Apr 18 15:57:46 2016 Z
   Check Point Endpoint Security - Full Disk Encryption v.7.5.100.25, 20160418
Mon Apr 18 15:57:15 2016 Z
   Cisco Systems VPN Client 5.0.07.0440 v.5.0.7, 20160418
Mon Apr 18 15:56:55 2016 Z
   Cisco AnyConnect Start Before Login Module v.3.1.05160, 20160418
Mon Apr 18 15:56:54 2016 Z
   Cisco AnyConnect Secure Mobility Client v.3.1.05160, 20160418
   Cisco AnyConnect Diagnostics and Reporting Tool v.3.1.05160, 20160418
Mon Apr 18 15:56:15 2016 Z
   WebEx Productivity Tools v.2.36.13053.10004, 20160418
Mon Apr 18 15:54:47 2016 Z
   WebEx Document Suite v.29.13.40.10011, 20160418
Mon Apr 18 15:54:46 2016 Z
   WebEx Support Manager for Internet Explorer v.29.13.40.10011, 20160418
Mon Apr 18 15:54:44 2016 Z
   WebEx Training Manager for Internet Explorer v.29.13.40.10011, 20160418
Mon Apr 18 15:54:43 2016 Z
   Network Recording Player v.29.13.40.10011, 20160418
Mon Apr 18 15:54:42 2016 Z
   Cisco WebEx Meeting Center for Internet Explorer v.29.13.41.10011, 20160418
Mon Apr 18 15:54:40 2016 Z
   WebEx Poll Questionnaire Editor v.29.13.30.10011, 20160418
Mon Apr 18 15:54:39 2016 Z
   WebEx Event Manager for Internet Explorer v.29.13.41.10011, 20160418
Mon Apr 18 15:54:25 2016 Z
   Java(TM) 6 Update 38 v.6.0.380, 20160418
                              Page 121

SOFTWARE OUTPUT.txt

Mon Apr 18 15:54:19 2016 Z
  SAFE Servlet v.7.05.00.219, 20160418
Mon Apr 18 15:54:07 2016 Z
  Java(TM) 6 Update 17 v.6.0.170, 20160418
Mon Apr 18 15:45:54 2016 Z
  WinZip 17.5 v.17.5.10480, 20160418
Mon Apr 18 15:45:31 2016 Z
  ActivClient x64 v.6.2, 20160418
Mon Apr 18 15:44:52 2016 Z
  Adobe Acrobat X Pro v.10.1.16, 20160418
Mon Apr 18 15:37:43 2016 Z
  DisplayLink Graphics v.7.9.665.0, 20160418
Mon Apr 18 15:37:38 2016 Z
  DisplayLink Core Software v.7.9.630.0, 20160418
Mon Apr 18 15:30:46 2016 Z
  Microsoft Policy Platform v.1.2.3602.0, 20160418
Mon Apr 18 15:30:36 2016 Z
  Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 v.12.0.21005,
20160418
  Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 v.12.0.21005,
20160418
  Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 v.12.0.21005, 20160418
Mon Apr 18 15:30:35 2016 Z
  Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 v.12.0.21005, 20160418
Mon Apr 18 15:28:10 2016 Z
  Realtek Audio COM Components v.1.0.2, 20160418
Wed Dec 30 13:27:50 2015 Z
  Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50908, 20151229
Wed Dec 30 12:24:51 2015 Z
  EMC SourceOne Offline Access v.6.72.0017, 20151230
Wed Dec 30 12:23:41 2015 Z
  Citrix online plug-in (HDX) v.12.1.0.30, 20151230
Wed Dec 30 12:23:40 2015 Z
  Citrix online plug-in (DV) v.12.1.0.30, 20151230
Wed Dec 30 12:23:38 2015 Z
  Citrix online plug-in (USB) v.12.1.0.30, 20151230
Wed Dec 30 12:23:31 2015 Z
  Citrix online plug-in (Web) v.12.1.0.30, 20151230
Wed Dec 30 12:23:18 2015 Z
  Access Card Utility v.1.4.2, 20151230
Wed Dec 30 12:20:19 2015 Z
  eRoom 7 Client v.503.196, 20151230
Wed Dec 30 10:06:56 2015 Z
  Microsoft Office Proof (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 09:57:50 2015 Z
  Microsoft Office OneNote MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 09:57:45 2015 Z
  Microsoft Office Office 64-bit Components 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 09:55:56 2015 Z
  Microsoft Office Word MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 09:55:53 2015 Z
  Microsoft Office Outlook MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 09:55:13 2015 Z
  Microsoft Office Shared MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 08:44:57 2015 Z
  Microsoft Office PowerPoint MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 08:44:54 2015 Z
  Microsoft Office Excel MUI (English) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 08:42:54 2015 Z
  Microsoft Office Proof (Spanish) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 08:42:51 2015 Z
  Microsoft Office Proof (French) 2010 v.14.0.7015.1000, 20151230
Wed Dec 30 07:06:36 2015 Z

Page 122

```
                         SOFTWARE OUTPUT.txt
   Microsoft Lync 2010 v.4.0.7577.4486, 20151230
Wed Dec 30 00:26:49 2015 Z
   Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010 v.14.0.7015.1000,
20151229
Wed Dec 30 00:26:47 2015 Z
   Microsoft Office Shared 64-bit MUI (English) 2010 v.14.0.7015.1000, 20151229
Wed Dec 30 00:26:28 2015 Z
   Microsoft Office Publisher MUI (English) 2010 v.14.0.7015.1000, 20151229
Wed Dec 30 00:26:25 2015 Z
   Microsoft Office Proofing (English) 2010 v.14.0.7015.1000, 20151229
Wed Dec 30 00:26:12 2015 Z
   Microsoft Office Shared Setup Metadata MUI (English) 2010 v.14.0.7015.1000,
20151229
Wed Dec 30 00:26:06 2015 Z
   Microsoft Office InfoPath MUI (English) 2010 v.14.0.7015.1000, 20151229
Wed Dec 30 00:26:02 2015 Z
   Microsoft Office Groove MUI (English) 2010 v.14.0.7015.1000, 20151229
Wed Dec 30 00:25:55 2015 Z
   Microsoft Office Access Setup Metadata MUI (English) 2010 v.14.0.7015.1000,
20151229
Wed Dec 30 00:25:52 2015 Z
   Microsoft Office Access MUI (English) 2010 v.14.0.7015.1000, 20151229
Tue Dec 29 18:27:34 2015 Z
   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 v.9.0.30729.6161,
20151229
Tue Dec 29 18:26:52 2015 Z
   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161,
20151229
Tue Dec 29 16:08:46 2015 Z
   Microsoft Office Live Meeting 2007 v.8.0.6362.91, 20151229
Tue Dec 29 16:06:55 2015 Z
   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148 v.9.0.30729.4148,
20151229
Tue Dec 29 16:05:49 2015 Z
   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148,
20151229

S-1-5-21-2431487851-277683799-2983902431-500
S-1-5-21-2431487851-277683799-2983902431-500\Products subkey not found.
-------------------------------------------
profilelist v.20100219
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList
LastWrite Time Tue Apr 19 20:02:50 2016 (UTC)

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : Tue Jul 14 04:53:25 2009 (UTC)

Path      : C:\Windows\ServiceProfiles\LocalService
SID       : S-1-5-19
LastWrite : Tue Dec 29 18:43:08 2015 (UTC)

Path      : C:\Windows\ServiceProfiles\NetworkService
SID       : S-1-5-20
LastWrite : Tue Dec 29 18:43:08 2015 (UTC)

Path      : C:\Users\ad_dcc_s.nchotu
SID       : S-1-5-21-1078081533-606747145-839522115-282625
LastWrite : Tue Apr 19 20:56:41 2016 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)
```

Page 123

```
                          SOFTWARE OUTPUT.txt
Path       : C:\Users\Abe-Arjun.Mallik
SID        : S-1-5-21-1078081533-606747145-839522115-317883
LastWrite  : Wed Apr 20 15:41:30 2016 (UTC)
LoadTime   : Thu Jan  1 00:00:00 1970 (UTC)

Path       : C:\Users\ad_dcc_d.pinckney
SID        : S-1-5-21-1078081533-606747145-839522115-320247
LastWrite  : Mon Apr 18 16:37:07 2016 (UTC)
LoadTime   : Thu Jan  1 00:00:00 1970 (UTC)

Path       : C:\Users\Administrator
SID        : S-1-5-21-2431487851-277683799-2983902431-500
LastWrite  : Mon Apr 18 15:26:54 2016 (UTC)
LoadTime   : Thu Jan  1 00:00:00 1970 (UTC)

Domain Accounts
----------------------------------------
regback v.20100219
(Software) List all tasks along with logfile name and last written date/time

regidle
Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Registry\RegIdleBackup
LastWrite: Tue Jul 14 04:54:36 2009

Id         {CA4B8FF2-A4D2-4D88-A52E-3A5BDAF7F56E}
Index      3
Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
LastWrite Time Thu Apr 28 15:00:38 2016 (UTC)

Path       :
\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
Dynamicinfo    : {01FC1385-88EB-4369-8FB2-FD5089B8CBEB}
LastWrite : Tue Dec 29 18:46:49 2015 (UTC)

Path           : \Microsoft\Windows\Time Synchronization\SynchronizeTime
Dynamicinfo    : {044A6734-E90E-4F8F-B357-B2DC8AB3B5EC}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path           : \OfficeSoftwareProtectionPlatform\SvcRestartTask
Dynamicinfo    : {04CB8DD4-0BFD-4CC6-9B78-E28FAFEE5706}
LastWrite : Tue Dec 29 15:52:23 2015 (UTC)

Path           : \Microsoft\Windows\SideShow\SessionAgent
Dynamicinfo    : {071A3D04-A86C-42B6-9AD1-B1097E70B26B}
LastWrite : Mon Apr 18 16:25:44 2016 (UTC)

Path           : \Microsoft\Windows\Tcpip\IpAddressConflict1
Dynamicinfo    : {088482FA-65B8-4E17-9ABF-1DCD48E8D373}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path           : \Microsoft\Windows\Tcpip\IpAddressConflict2
Dynamicinfo    : {09F06BFE-A3C8-40E3-846A-6E6F4000C238}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path           : \GoogleUpdateTaskMachineCore
Dynamicinfo    : {12ED6126-B2FE-4078-9D4C-D38B27165E5B}
LastWrite : Thu Apr 28 15:00:41 2016 (UTC)

Path           : \Microsoft\Windows\SideShow\AutoWake
Dynamicinfo    : {151FAFA1-7797-4589-BF05-B3B38E5F5601}
LastWrite : Tue Dec 29 18:46:50 2015 (UTC)
```

Page 124

```
                              SOFTWARE OUTPUT.txt
Path               : \GoogleUpdateTaskMachineUA
Dynamicinfo        : {17985626-25F9-4262-A556-462743C375C7}
LastWrite : Thu Apr 28 15:00:44 2016 (UTC)

Path               : \Microsoft\Windows\Task Manager\Interactive
Dynamicinfo        : {1F7B7221-AE8F-44F3-BA82-F7D260F51964}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\Multimedia\SystemSoundsService
Dynamicinfo        : {2470470F-2634-478E-B181-571E98A789BB}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\Active Directory Rights Management Services
Client\AD RMS Rights Policy Template Management (Manual)
Dynamicinfo        : {28011108-68DF-4C73-B91B-57427D501BBA}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\Application Experience\Microsoft Compatibility
Appraiser
Dynamicinfo        : {2C54FEED-8EB3-44C1-90DA-F346E8730A98}
LastWrite : Wed Apr 20 16:11:50 2016 (UTC)

Path               : \Microsoft\Configuration Manager\Configuration Manager Health
Evaluation
Dynamicinfo        : {2CFB0203-95F1-4251-9E8A-FAE9DFEE08FF}
LastWrite : Thu Apr 28 15:00:57 2016 (UTC)

Path               : \Microsoft\Windows\WindowsBackup\ConfigNotification
Dynamicinfo        : {2F57269B-1E09-4E2D-AB1E-B0FDAC7D279C}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\MobilePC\HotStart
Dynamicinfo        : {37602615-6E33-4F47-8789-4CCA300D56E2}
LastWrite : Tue Dec 29 18:46:54 2015 (UTC)

Path               : \RtHDVBg_PushButton
Dynamicinfo        : {44293E25-EF4E-464E-962E-09AA1F7B7452}
LastWrite : Wed Apr 20 15:42:01 2016 (UTC)

Path               : \Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
Dynamicinfo        : {47536D45-EEEC-4BDC-8183-A4DC1F8DA9E4}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\Shell\WindowsParentalControlsMigration
Dynamicinfo        : {486D715E-6AA2-44CF-BC48-B6990CBB53C6}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Windows\TextServicesFramework\MsCtfMonitor
Dynamicinfo        : {4C8B01A2-11FF-4C41-848F-508EF4F00CF7}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path               : \Microsoft\Configuration Manager\Configuration Manager Idle
Detection
Dynamicinfo        : {4E67C660-6EE4-4F90-8169-A25F60782DF4}
LastWrite : Wed Apr 20 16:26:34 2016 (UTC)

Path               : \Microsoft\Windows\TabletPC\InputPersonalization
Dynamicinfo        : {5A0D8346-8352-4FB9-9735-0507DE07A603}
LastWrite : Mon Apr 18 15:31:59 2016 (UTC)

Path               : \Microsoft\Windows\UPnP\UPnPHostConfig
Dynamicinfo        : {5A40E926-9E86-4B89-9CFD-B12311724371}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
                              Page 125
```

SOFTWARE OUTPUT.txt

```
Path          : \Microsoft\Windows\Shell\WindowsParentalControls
Dynamicinfo   : {5B42DD9C-5A26-4F27-BB95-34603F0997E5}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Defrag\ScheduledDefrag
Dynamicinfo   : {5C0AEEEA-C154-45BE-8499-BEA5F11BAFF6}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\CertificateServicesClient\SystemTask
Dynamicinfo   : {5F5A18EB-DC73-4E45-A11C-B59043598412}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Active Directory Rights Management Services
Client\AD RMS Rights Policy Template Management (Automated)
Dynamicinfo   : {613612BA-897D-44CE-8DC1-8FC283F9FD51}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Adobe Acrobat Update Task
Dynamicinfo   : {634E1AE3-00D0-4079-8D2A-FD85C8819ECA}
LastWrite : Thu Apr 28 15:00:36 2016 (UTC)

Path          : \Microsoft\Windows\Windows Activation
Technologies\ValidationTaskDeadline
Dynamicinfo   : {640C5CDC-9131-4892-B2B1-6FF157EE98B3}
LastWrite : Mon Apr 18 15:32:53 2016 (UTC)

Path          : \Microsoft\Windows\User Profile Service\HiveUploadTask
Dynamicinfo   : {6738BA6E-EA75-4B6B-B8B8-71F0336DD8EF}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\SideShow\GadgetManager
Dynamicinfo   : {7109364A-94BE-4481-AEB4-7993D9AD5DBA}
LastWrite : Tue Dec 29 18:46:51 2015 (UTC)

Path          : \Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck
Dynamicinfo   : {72DB7465-BC54-491B-A92A-4637A28C9BBF}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          :
\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
Dynamicinfo   : {73F215EA-F160-438C-BE0A-A13BDCE5C106}
LastWrite : Tue Dec 29 18:46:49 2015 (UTC)

Path          : \Microsoft\Windows\Windows Media Sharing\UpdateLibrary
Dynamicinfo   : {753C47AE-EC5E-44B3-95A9-2C8E553F0E39}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\CertificateServicesClient\UserTask
Dynamicinfo   : {7AFCC0CA-7121-422A-AB45-B0E8D599FF08}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\NetTrace\GatherNetworkInfo
Dynamicinfo   : {81540B9F-B5BF-47EB-9C95-BE195BF2C664}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Windows Activation Technologies\ValidationTask
Dynamicinfo   : {882167B6-ED90-4AD7-BCC8-BB8F8D4021D0}
LastWrite : Mon Apr 18 15:32:53 2016 (UTC)

Path          : \UDI_cleanup
Dynamicinfo   : {91ECAF68-6A1F-496C-A81A-950F801F1056}
LastWrite : Mon Apr 18 16:05:05 2016 (UTC)
```

Page 126

SOFTWARE OUTPUT.txt

```
Path          : \Microsoft\Windows\WDI\ResolutionHost
Dynamicinfo   : {9435F817-FED2-454E-88CD-7F78FDA62C48}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Adobe Flash Player Updater
Dynamicinfo   : {94E5F234-AC7A-4AAD-8C45-E1FD63BBD7E2}
LastWrite : Thu Apr 28 15:00:44 2016 (UTC)

Path          : \Microsoft\Windows\SystemRestore\SR
Dynamicinfo   : {994C86AD-A929-4B2C-88A0-4E25A107A029}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\CertificateServicesClient\UserTask-Roam
Dynamicinfo   : {9979CB83-103A-4105-9E5D-C74B0AF6D198}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Offline Files\Background Synchronization
Dynamicinfo   : {A2D82D31-17C4-46B9-8B3A-B3330A172C80}
LastWrite : Tue Dec 29 15:49:22 2015 (UTC)

Path          : \Microsoft\Windows\WindowsColorSystem\Calibration Loader
Dynamicinfo   : {A35BB7A6-5F0C-4C9F-8450-2B3BED532D51}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\AppID\PolicyConverter
Dynamicinfo   : {A48CABBF-24C8-4B87-B00F-9261807C3B43}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Location\Notifications
Dynamicinfo   : {A6AF9377-77CE-47AB-AD7D-EC32CAD0C82D}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Application Experience\AitAgent
Dynamicinfo   : {AC4E5ACF-89F7-4220-BA21-81EE183975E2}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Ras\MobilityManager
Dynamicinfo   : {AC668097-4D6B-4093-AC14-014C09DBF820}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\PerfTrack\BackgroundConfigSurveyor
Dynamicinfo   : {B0CBAB43-44FC-469B-A4CE-87426761FDCE}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\SideShow\SystemDataProviders
Dynamicinfo   : {BB5C8A8B-8D46-4455-B555-849754F66089}
LastWrite : Mon Apr 18 16:25:59 2016 (UTC)

Path          : \Microsoft\Windows\Diagnosis\Scheduled
Dynamicinfo   : {BE669C13-8165-4536-96D0-6D6C39292AAE}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \Microsoft\Windows\Customer Experience Improvement
Program\Consolidator
Dynamicinfo   : {C016366B-7126-46CA-B36B-592A3D95A60B}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path          : \UDI_Regcleanup
Dynamicinfo   : {C988DD3B-0D50-4D9B-B65B-A8724F9C43C0}
LastWrite : Mon Apr 18 16:05:06 2016 (UTC)

Path          : \Microsoft\Windows\Registry\RegIdleBackup
```
Page 127

SOFTWARE OUTPUT.txt
DynamicInfo : {CA48BFF2-A4D2-4D88-A52E-3A5BDAF7F56E}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask
DynamicInfo : {CB3D64BF-C0C9-45FF-BF80-FF1A8F680186}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\MemoryDiagnostic\CorruptionDetector
DynamicInfo : {CEE6455B-E1A7-4D9D-80A7-2001912BE5B5}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\Error Reporting\QueueReporting
DynamicInfo : {D0250F3F-6480-484F-B719-42F659AC64D5}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\Wininet\CacheTask
DynamicInfo : {D513DAC7-E6AB-4916-95E4-EDF4E721DE41}
LastWrite : Mon Apr 18 15:51:14 2016 (UTC)
Path : \Microsoft\Windows\Autochk\Proxy
DynamicInfo : {D7B6E81D-3CF4-432C-84DC-24213F4316E6}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\Maintenance\WinSAT
DynamicInfo : {DA41DE71-8431-42FB-9DB0-EB64A961DEAD}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask
DynamicInfo : {DD9F510C-95F4-499A-90C8-BAC5B8C372FF4}
LastWrite : Wed Apr 20 16:42:11 2016 (UTC)
Path : \Microsoft\Windows Filtering Platform\BfeOnServiceStartTypeChange
DynamicInfo : {E22A8667-F75B-4BA9-BA46-067ED4429DE8}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\Bluetooth\UninstallDeviceTask
DynamicInfo : {E3163C33-301D-4730-A266-5518C5ED3967}
LastWrite : Sun Nov 21 03:39:16 2010 (UTC)
Path : \Microsoft\Windows\RAC\RacTask
DynamicInfo : {EACA24FF-236C-401D-A1E7-B3D5267B8A50}
LastWrite : Sun Nov 21 03:39:16 2010 (UTC)
Path : \Microsoft\Windows\MUI\LPRemove
DynamicInfo : {EB02381F-D652-4B1C-894A-712498C62C51}
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)
Path : \Microsoft\Windows\Offline Files\Logon Synchronization
DynamicInfo : {F6F015F2-84F2-4A56-807D-475B9CEA3625}
LastWrite : Tue Dec 29 18:46:48 2015 (UTC)
Path : \Microsoft\Windows\Application Experience\ProgramDataUpdater
DynamicInfo : {F7C1C47A-44A2-45A6-BA57-4506F0CD8AF0}
LastWrite : Wed Dec 30 07:45:33 2015 (UTC)
Path : \Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
DynamicInfo : {FA2BC0A6-8D4B-458A-85C8-2B8C72487513}
LastWrite : Sun Nov 21 03:39:16 2010 (UTC)
Path : \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
DynamicInfo : {FB3C354D-297A-4EB2-9B58-090F6361906B}
LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

Page 128

SOFTWARE OUTPUT.txt

```
Path           : \Microsoft\Windows\Customer Experience Improvement
Program\KernelCeipTask
Dynamicinfo    : {FDD56C73-F0D5-41B6-B767-6EFFD7966428}
LastWrite : Sun Nov 21 03:39:16 2010 (UTC)


------------------------------------------
removdev v.200800611
(Software) Parses Windows Portable Devices key (Vista)

RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Tue Apr 19 19:48:27 2016 (UTC)

Device     : DISK&VEN_&PROD_&REV_8.07
LastWrite : Tue Apr 19 19:48:27 2016 (UTC)
SN         : B57D6A2F&0
Drive      : Configuration Manager 2012


------------------------------------------
renocide v.20130425
(Software) Check for Renocide malware

Microsoft\DRM\amty not found.
------------------------------------------
schedagent v.20100817
(Software) Get SchedulingAgent key contents

Microsoft\SchedulingAgent
LastWrite Time Tue Jul 14 05:08:49 2009 (UTC)

OldName       = 37L4247E29-32
LogPath       = %SystemRoot%\Tasks\SCHEDLGU.TXT
MaxLogSizeKB = 32
TasksFolder   = %SystemRoot%\Tasks
------------------------------------------
secctr v.20100310
(Software) Get data from Security Center key

secctr


Microsoft\Security Center
LastWrite Time Wed Apr 20 15:43:10 2016 (UTC)

cval                    0x01
------------------------------------------
sfc v.20100305
(Software) Get SFC values

sfc v.20100305

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Wed Apr 20 15:40:55 2016 (UTC)


Policies\Microsoft\Windows NT\Windows File Protection
LastWrite Time Tue Jul 14 04:49:20 2009 (UTC)

------------------------------------------
shellexec v.20130410
(Software) Gets ShellExecuteHooks from Software hive
```

Page 129

```
                          SOFTWARE OUTPUT.txt
Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
LastWrite Time Tue Dec 29 15:52:10 2015 (UTC)


{B5A7F190-DDA6-4420-B3BA-52453494E6CD}
   Class     => Groove GFS Stub Execution Hook
   Module    => C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   LastWrite => Tue Dec 29 15:52:07 2015

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
LastWrite Time Tue Dec 29 15:55:12 2015 (UTC)


{B5A7F190-DDA6-4420-B3BA-52453494E6CD}
   Class     => Groove GFS Stub Execution Hook
   Module    => C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   LastWrite => Tue Dec 29 15:52:07 2015


------------------------------------------
shellext v.20100515
(Software) Gets Shell Extensions from Software hive

Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
LastWrite Time Mon Apr 18 15:50:45 2016 (UTC)

{2916C86E-86A6-43FE-8112-43ABE6BF8DCC}  Groove Explorer Icon Overlay 4 (GFS Unread
Mark)
   DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}  Groove GFS Browser Helper
   DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97}  Microsoft Office Thumbnail Handler
   DLL: C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{920E6DB1-9907-4370-B3A0-BAFC03D81399}  Groove Explorer Icon Overlay 2.5 (GFS Unread
Folder)
   DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{00C6D95F-329C-409a-81D7-C46C66EA7F33}
   DLL: %SystemRoot%\System32\shdocvw.dll
   Timestamp: Tue Apr 12 07:45:34 2011 Z

{E0D79306-84BE-11CE-9641-444553540000}  WinZip
   DLL: C:\Program Files\WinZip\wzshls64.dll
   Timestamp: Mon Apr 18 15:45:53 2016 Z

{A929C4CE-FD36-4270-B4F5-34ECAC5BD63C}  NvAppShExt extension
   DLL: C:\WINDOWS\system32\nv3dappshext.dll
   Timestamp: Mon Apr 18 15:28:47 2016 Z

{99FD978C-D287-4F50-827F-B2C658EDA8E7}  Groove Explorer Icon Overlay 1 (GFS Unread
Stub)
   DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{3D60EDA7-9AB4-4DA8-864C-D9B5F2E7281D}  Groove Namespace Extension
   DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
   Timestamp: Tue Dec 29 15:52:07 2015 Z

{0875DCB6-C686-4243-9432-ADCCF0B9F2D7}  Microsoft OneNote Namespace Extension for
                                  Page 130
```

SOFTWARE OUTPUT.txt

Windows Desktop Search
    DLL: C:\Program Files\Microsoft Office\Office14\ONFILTER.DLL
    Timestamp: Tue Dec 29 15:52:07 2015 Z

{80009818-f38f-4af1-87b5-eadab9433e58}  MF ADTS Property Handler
    DLL: %SystemRoot%\System32\mf.dll
    Timestamp: Tue Jul 14 04:53:38 2009 Z

{42042206-2D85-11D3-8CFF-005004838597}  Microsoft Office HTML Icon Handler
    DLL: C:\Program Files\Microsoft Office\Office14\MSOHEVI.DLL
    Timestamp: Tue Dec 29 15:52:07 2015 Z

{E97DEC16-A50D-49bb-AE24-CF682282E08D}  OpenGLShExt extension
    DLL: C:\WINDOWS\system32\nv3dappshext.dll
    Timestamp: Mon Apr 18 15:28:47 2016 Z

{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE}  Subscription Mgr
    DLL: C:\Windows\System32\webcheck.dll
    Timestamp: Mon Apr 18 15:51:11 2016 Z

{E0D79304-84BE-11CE-9641-444553540000}  WinZip
    DLL: C:\Program Files\WinZip\wzshls64.dll
    Timestamp: Mon Apr 18 15:45:53 2016 Z

{D66DC78C-4F61-447F-942B-3FB6980118CF}  {D66DC78C-4F61-447F-942B-3FB6980118CF}
    DLL: C:\Program Files\Microsoft Office\Office14\VISSHE.DLL
    Timestamp: Tue Dec 29 15:52:08 2015 Z

{F5175861-2688-11d0-9C5E-00AA00A45957}  Subscription Folder
    DLL: C:\Windows\System32\webcheck.dll
    Timestamp: Mon Apr 18 15:51:11 2016 Z

{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}  Microsoft Office Metadata Handler
    DLL: C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll
    Timestamp: Tue Dec 29 15:52:07 2015 Z

{E0D79307-84BE-11CE-9641-444553540000}  WinZip
    DLL: C:\Program Files\WinZip\wzshls64.dll
    Timestamp: Mon Apr 18 15:45:53 2016 Z

{08165EA0-E946-11CF-9C87-00AA005127ED}  WebCheckWebCrawler
    DLL: C:\Windows\System32\webcheck.dll
    Timestamp: Mon Apr 18 15:51:11 2016 Z

{506F4668-F13E-4AA1-BB04-B43203AB3CC0}  {506F4668-F13E-4AA1-BB04-B43203AB3CC0}
    DLL: C:\Program Files\Microsoft Office\Office14\VISSHE.DLL
    Timestamp: Tue Dec 29 15:52:08 2015 Z

{C612F052-C85C-4156-B974-87947FAA7569}  SMS Application Publisher
    DLL: C:\WINDOWS\CCM\SMSARPPub.dll
    Timestamp: Tue Apr 19 20:00:01 2016 Z

{B5A7F190-DDA6-4420-B3BA-52453494E6CD}  Groove GFS Stub Execution Hook
    DLL: C:\PROGRA~1\MICROS~1\Office14\GROOVEEX.DLL
    Timestamp: Tue Dec 29 15:52:07 2015 Z

{D25B2CAB-8A9A-4517-A9B2-CB5F68A5A802}  Adobe.Acrobat.ContextMenu
    DLL: C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\..\Acrobat
Elements\ContextMenu64.dll
    Timestamp: Mon Apr 18 15:44:51 2016 Z

{7D559C10-9FE9-11d0-93F7-00AA0059CE02}  Code Download Agent
    DLL: C:\Windows\System32\webcheck.dll

Page 131

```
                        SOFTWARE OUTPUT.txt
  Timestamp: Mon Apr 18 15:51:11 2016 Z


{6C467336-8281-4E60-8204-430CED96822D}  Groove GFS Context Menu Handler
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z


{16F3DD56-1AF5-4347-846D-7C10C4192619}  Groove Explorer Icon Overlay 3 (GFS Folder)
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z


{387E725D-DC16-4D76-B310-2C93ED4752A0}  Groove XML Icon Handler
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z


{2A541AE1-5BF6-4665-A8A3-CFA9672E4291}  Groove GFS Explorer Bar
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z


{A70C977A-BF00-412C-90B7-034C51DA2439}  NvCpl DesktopContext Class
  DLL: C:\Program Files\NVIDIA Corporation\Display\nvui.dll
  Timestamp: Mon Apr 18 15:28:47 2016 Z


{E6FB5E20-DE35-11CF-9C87-00AA005127ED}  WebCheck
  DLL:
  Timestamp: Thu Jan  1 00:00:00 1970 Z


{0006F045-0000-0000-C000-000000000046}  Microsoft Outlook Custom Icon Handler
  DLL: C:\Program Files\Microsoft Office\Office14\OLKFSTUB.DLL
  Timestamp: Tue Dec 29 15:52:08 2015 Z


{E0D79305-84BE-11CE-9641-444553540000}  WinZip
  DLL: C:\Program Files\WinZip\wzshls64.dll
  Timestamp: Mon Apr 18 15:45:53 2016 Z


{AB5C5600-7E6E-4B06-9197-9ECEF74D31CC}  Groove Explorer Icon Overlay 2 (GFS Stub)
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z


{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB}  WebCheck SyncMgr Handler
  DLL: C:\Windows\System32\webcheck.dll
  Timestamp: Mon Apr 18 15:51:11 2016 Z


{3D1975AF-48C6-4f8e-A182-BE0E08FA86A9}  NVIDIA Play On My TV Context Menu Extension
  DLL: %SystemRoot%\system32\nvshext.dll
  Timestamp: Mon Apr 18 15:28:47 2016 Z


{7CCA70DB-DE7A-4FB7-9B2B-52E2335A3B5A}  Nameext
  DLL: C:\Program Files\Microsoft Office\Office14\NAMEEXT.DLL
  Timestamp: Tue Dec 29 15:52:08 2015 Z


{A449600E-1DC6-4232-B948-9BD794D62056}  Groove GFS Stub Icon Handler
  DLL: C:\PROGRA~1\MICROS~1\office14\GROOVEEX.DLL
  Timestamp: Tue Dec 29 15:52:07 2015 Z

-------------------------------------------
shelloverlay v.20100308
(Software) Gets ShellIconOverlayIdentifiers values

shelloverlay
Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
LastWrite Time Tue Dec 29 15:52:10 2015 (UTC)

Tue Dec 29 15:52:10 2015 Z
```

Page 132

SOFTWARE OUTPUT.txt
  Groove Explorer Icon Overlay 1 (GFS Unread Stub)
{99FD978C-D287-4F50-827F-B2C658EDA8E7}
    Groove Explorer Icon Overlay 2 (GFS Stub)   {AB5C5600-7E6E-4B06-9197-9ECEF74D31CC}
    Groove Explorer Icon Overlay 2.5 (GFS Unread Folder)
{920E6DB1-9907-4370-B3A0-BAFC03D81399}
    Groove Explorer Icon Overlay 3 (GFS Folder)
{16F3DD56-1AF5-4347-846D-7C10C4192619}
    Groove Explorer Icon Overlay 4 (GFS Unread Mark)
{2916C86E-86A6-43FE-8112-43ABE6BF8DCC}


Tue Apr 12 07:45:22 2011 Z
  Offline Files   {4E77131D-3629-431c-9818-C5679DC83E81}


Tue Jul 14 04:53:25 2009 Z
  EnhancedStorageShell   {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}
  SharingPrivate   {08244EE6-92F0-47f2-9FC9-929BAA2E7235}


-------------------------------------------
snapshot v.20080725
(Software) Check ActiveX comp kill bit; Access Snapshot

ActiveX Snapshot Vuln
Microsoft\Internet Explorer

IE Version = 9.11.9600.18163


GUID: {F0E42D50-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400


GUID: {F0E42D60-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400


GUID: {F2175210-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400


-------------------------------------------
soft_run v.20130603
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Mon Apr 18 16:05:05 2016 (UTC)
  RtHDVBg_MAXX6 - "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /MAXX6
/WAVES_SUBTYPE_FOR_LYNC
  accrdsub - "C:\Program Files\ActivIdentity\ActivClient\accrdsub.exe"
  RunAppInstall - C:\WINDOWS\UDI\AppInstall.exe
  acevents - "C:\Program Files\ActivIdentity\ActivClient\acevents.exe"
  RtHDVCpl - "C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" /s
  McAfee Host Intrusion Prevention Tray - "C:\Program Files\McAfee\Host Intrusion
Prevention\FireTray.exe"
  Apoint - C:\Program Files\DellTPad\Apoint.exe

Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Wed Apr 20 15:39:52 2016 (UTC)
  MSKSSRV - rundll32.exe streamci,StreamingDeviceSetup
{96E080C7-143C-11D1-B40F-00A0C9223196},{3C0D501A-140B-11D1-B40F-00A0C9223196},{3C0D5
01A-140B-11D1-B40F-00A0C9223196}
  MSPCLOCK - rundll32.exe streamci,StreamingDeviceSetup
{97ebaacc-95bd-11d0-a3ea-00a0c9223196},{53172480-4791-11D0-A5D6-28DB04C10000},{53172
480-4791-11D0-A5D6-28DB04C10000}
  MSPQM - rundll32.exe streamci,StreamingDeviceSetup
{DDF4358E-BB2C-11D0-A42F-00A0C9223196},{97EBAACB-95BD-11D0-A3EA-00A0C9223196},{97EBA
Page 133

SOFTWARE OUTPUT.txt
ACB-95BD-11D0-A3EA-00A0C9223196}
   MSTEE.CxTransform - rundll32.exe streamci,StreamingDeviceSetup
{cfd669f1-9bc2-11d0-8299-0000f822fe8a},{CF1DDA2C-9743-11D0-A3EE-00A0C9223196},{CF1DD
A2C-9743-11D0-A3EE-00A0C9223196},C:\WINDOWS\inf\ksfilter.inf,MSTEE.Interface.Install
   MSTEE.Splitter - rundll32.exe streamci,StreamingDeviceSetup
{cfd669f1-9bc2-11d0-8299-0000f822fe8a},{0A4252A0-7E70-11D0-A5D6-28DB04C10000},{0A425
2A0-7E70-11D0-A5D6-28DB04C10000},C:\WINDOWS\inf\ksfilter.inf,MSTEE.Interface.Install
   WDM_DRMKAUD - rundll32.exe streamci,StreamingDeviceSetup
{EEC12DB6-AD9C-4168-8658-B03DAEF417FE},{ABD61E00-9350-47e2-A632-4438B90C6641},{FFBB6
E3F-CCFE-4D84-90D9-421418B03A8E},C:\WINDOWS\inf\WDMAUDIO.inf,WDM_DRMKAUD.Interface.I
nstall

Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Wed Apr 20 13:19:03 2016 (UTC)
   ShStatEXE - "C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE"
/STANDALONE
   Cisco AnyConnect Secure Mobility Agent for Windows - "C:\Program Files
(x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe" -autolaunched
   Adobe Acrobat Speed Launcher - "C:\Program Files (x86)\Adobe\Acrobat
10.0\Acrobat\Acrobat_sl.exe"
   SunJavaUpdateSched - "C:\Program Files (x86)\Java\jre6\bin\jusched.exe"
   ConnectionCenter - "C:\Program Files (x86)\Citrix\ICA Client\concentr.exe"
/startup
   McAfeeUpdaterUI - "C:\Program Files (x86)\McAfee\Common
Framework\x86\UpdaterUI.exe" /StartedFromRunKey
   BCSSync - "C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe"
/DelayServices
   Pointsec Tray - C:\Program Files (x86)\Pointsec\Pointsec for PC\P95Tray.exe
   Communicator - "C:\Program Files (x86)\Microsoft Lync\communicator.exe"
/fromrunkey
   Acrobat Assistant 8.0 - "C:\Program Files (x86)\Adobe\Acrobat
10.0\Acrobat\Acrotray.exe"
   Check Point Endpoint Tray Application - C:\Program Files (x86)\Common Files\Check
Point\UIFramework\cptray.exe


Wow6432Node\Microsoft\Windows\CurrentVersion\Run\OptionalComponents
LastWrite Time Mon Apr 18 15:44:18 2016 (UTC)

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Mon Apr 18 16:26:01 2016 (UTC)
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

-------------------------------------------
spp_clients v.20130429
(Software) Determines volumes monitored by VSS

SPP_Clients
                              Page 134

SOFTWARE OUTPUT.txt
Microsoft\Windows NT\CurrentVersion\SPP\Clients
LastWrite Time Sun Nov 21 03:58:28 2010 (UTC)

----------------------------------------
sql_lastconnect v.20090112
(Software) MDAC cache of successful connections

Microsoft\MSSQLServer\Client\SuperSocketNetLib\LastConnect
MDAC Cache of successful connections
LastWrite Time Mon Apr 18 15:26:54 2016 (UTC)

BVTSQL1             84672521:tcp:BVTSQL1,1433
----------------------------------------
ssid v.20100301
(Software) Get WZCSVC SSID Info

Microsoft\WZCSVC\Parameters\Interfaces not found.
Microsoft\EAPOL\Parameters\Interfaces not found.
----------------------------------------
startmenuinternetapps_lm v.20101219
(SOFTWARE) Start Menu Internet Applications info

Start Menu Internet Applications


 [Tue Dec 29 15:55:13 2015 (UTC)] Calendar
 VALUE: (default) -> Microsoft Outlook
 SUBKEY:  [Tue Dec 29 15:55:12 2015 (UTC)] Microsoft Outlook


 [Tue Dec 29 15:55:13 2015 (UTC)] Contacts
 VALUE: (default) -> Microsoft Outlook
 SUBKEY:  [Tue Jul 14 04:55:00 2009 (UTC)] Address Book
 SUBKEY:  [Tue Dec 29 15:55:12 2015 (UTC)] Microsoft Outlook


 [Tue Dec 29 15:55:13 2015 (UTC)] EnvelopeHost
 VALUE: no values.
 SUBKEY:  [Tue Dec 29 15:55:12 2015 (UTC)] Microsoft Access
 SUBKEY:  [Tue Dec 29 15:55:12 2015 (UTC)] Microsoft Excel
 SUBKEY:  [Tue Dec 29 15:55:13 2015 (UTC)] Microsoft Publisher
 SUBKEY:  [Tue Dec 29 15:55:13 2015 (UTC)] Microsoft Word


 [Mon Apr 18 15:50:45 2016 (UTC)] Mail
 VALUE: (default) -> Microsoft Outlook
 SUBKEY:  [Tue Dec 29 15:55:13 2015 (UTC)] Microsoft Outlook
 SUBKEY:  [Mon Apr 18 15:29:26 2016 (UTC)] Windows Mail


 [Wed Dec 30 12:48:40 2015 (UTC)] Media
 VALUE: no values.
 SUBKEY:  [Tue Jul 14 04:55:00 2009 (UTC)] Windows Media Player


 [Mon Apr 18 15:29:26 2016 (UTC)] News
 VALUE: no values.
 SUBKEY:  [Mon Apr 18 15:29:26 2016 (UTC)] Windows Mail


 [Tue Dec 29 18:43:51 2015 (UTC)] Note taking
 VALUE: no values.
 SUBKEY:  [Tue Dec 29 18:43:51 2015 (UTC)] Microsoft OneNote
                         Page 135

SOFTWARE OUTPUT.txt

[Tue Dec 29 18:43:51 2015 (UTC)] Presentation
VALUE: no values.
SUBKEY:   [Tue Dec 29 18:43:51 2015 (UTC)] Microsoft PowerPoint


[Tue Dec 29 18:43:51 2015 (UTC)] Publishing
VALUE: no values.
SUBKEY:   [Tue Dec 29 18:43:51 2015 (UTC)] Microsoft Publisher


[Tue Dec 29 18:43:51 2015 (UTC)] Spreadsheet
VALUE: no values.
SUBKEY:   [Tue Dec 29 18:43:51 2015 (UTC)] Microsoft Excel


[Tue Apr 19 20:41:00 2016 (UTC)] StartMenuInternet
VALUE: (default) -> IEXPLORE.EXE
SUBKEY:   [Tue Apr 19 20:40:52 2016 (UTC)] FIREFOX.EXE
SUBKEY:   [Tue Apr 19 20:41:00 2016 (UTC)] Google Chrome
SUBKEY:   [Mon Apr 18 15:50:45 2016 (UTC)] IEXPLORE.EXE


[Tue Dec 29 18:43:51 2015 (UTC)] Word processing
VALUE: no values.
SUBKEY:   [Tue Dec 29 18:43:51 2015 (UTC)] Microsoft Word
----------------------------------------
svchost v.20100322
(Software) Get entries from SvcHost key

svchost


Microsoft\Windows NT\CurrentVersion\SvcHost
LastWrite Time Wed Dec 30 12:48:40 2015 (UTC)

RPCSS            RpcEptMapper,RpcSs
defragsvc        defragsvc
LocalSystemNetworkRestricted
UxSms,WdiSystemHost,Netman,trkwks,AudioEndpointBuilder,WUDFSvc,IPBusEnum,hidserv,dot
3svc,irmon,sysmain,PcaSvc,homegrouplistener,WPDBusEnum,wlansvc,TabletInputService,Cs
cService,UmRdpService,StorSvc
LocalService
nsi,WdiServiceHost,w32time,EventSystem,RemoteRegistry,WinHttpAutoProxySvc,sppuinotif
y,THREADORDER,netprofm,lltdsvc,fdphost,SstpSvc,WebClient,FontCache
netsvcs
AeLookupSvc,CertPropSvc,SCPolicySvc,lanmanserver,gpsvc,IKEEXT,AudioSrv,FastUserSwitc
hingCompatibility,Ias,Irmon,Nla,Ntmssvc,NWCWorkstation,Nwsapagent,Rasauto,Rasman,Rem
oteaccess,SENS,Sharedaccess,SRService,Tapisrv,Wmi,WmdmPmSp,TermService,wuauserv,BITS
,ShellHWDetection,LogonHours,PCAudit,helpsvc,uploadmgr,iphlpsvc,seclogon,AppInfo,msi
scsi,MMCSS,winmgmt,SessionEnv,browser,EapHost,schedule,hkmsvc,wercplsupport,ProfSvc,
Themes,BDESVC,AppMgmt
WerSvcGroup      wersvc
LocalServiceNoNetwork DPS,PLA,BFE,mpssvc,WwanSvc
termsvcs         TermService
swprv            swprv
LocalServiceNetworkRestricted
DHCP,eventlog,AudioSrv,BthHFSrv,LmHosts,wscsvc,homegroupprovider,WPCSvc
LocalServicePeerNet PNRPSvc,p2pimsvc,p2psvc,PnrpAutoReg
NetworkServiceAndNoImpersonation KtmRm

regsvc           RemoteRegistry
                              Page 136

SOFTWARE OUTPUT.txt
LocalServiceAndNoImpersonation
SSDPSRV,upnphost,SCardSvr,TBS,fdrespub,AppIDSvc,QWAVE,wcncsvc,SensrSvc
DcomLaunch          Power,PlugPlay,DcomLaunch
NetworkServiceNetworkRestricted PolicyAgent

NetworkService
CryptSvc,DHCP,TermService,DNSCache,lanmanworkstation,NapAgent,nlasvc,WinRM,WECSVC,Ta
pisrv
sdrsvc              sdrsvc
WbioSvcGroup        WbioSrvc
imgsvc              StiSvc
wcssvc              WcsPlugInService
AxInstSVGroup       AxInstSV
secsvcs             WinDefend
bthsvcs             bthserv
PeerDist            PeerDistSvc
utcsvc              DiagTrack
GPSvcGroup          GPSvc
-------------------------------------------
Launching tracing v.20120509
Microsoft\Tracing
Mon Apr 18 15:26:54 2016    cmd_RASAPI32
Mon Apr 18 15:26:54 2016    cmd_RASMANCS
Mon Apr 18 15:26:54 2016    Explorer_RASAPI32
Tue Apr 19 20:46:10 2016    Explorer_RASDLG
Tue Apr 19 20:46:13 2016    Explorer_RASGCW
Mon Apr 18 15:26:54 2016    Explorer_RASMANCS
Mon Apr 18 15:26:54 2016    IENRCORE_RASAPI32
Mon Apr 18 15:26:54 2016    IENRCORE_RASMANCS
Tue Jul 14 05:08:52 2009    IpHlpSvc
Mon Apr 18 16:26:11 2016    KMDDSP
Tue Apr 19 20:03:27 2016    mighost_RASAPI32
Tue Apr 19 20:03:28 2016    mighost_RASMANCS
Mon Apr 18 16:26:11 2016    NDPTSP
Mon Apr 18 16:26:11 2016    PPP
Mon Apr 18 16:26:11 2016    RASCCP
Mon Apr 18 16:26:11 2016    RASEAP
Mon Apr 18 16:26:11 2016    RASIPCP
Mon Apr 18 16:26:11 2016    RASIPHLP
Mon Apr 18 16:26:11 2016    RASIPV6CP
Mon Apr 18 16:26:11 2016    RASMAN
Mon Apr 18 16:26:11 2016    RASPAP
Tue Jul 14 05:01:47 2009    RASPLAP
Mon Apr 18 16:26:11 2016    RASTAPI
Mon Apr 18 16:37:10 2016    svchost_RASAPI32
Mon Apr 18 16:26:11 2016    svchost_RASCHAP
Tue Jul 14 05:09:58 2009    svchost_RASDLG
Tue Apr 19 19:53:07 2016    svchost_RASMANCS
Mon Apr 18 16:17:28 2016    svchost_RASTLS
Mon Apr 18 16:26:11 2016    tapi32
Mon Apr 18 16:26:11 2016    tapisrv
Mon Apr 18 16:26:11 2016    VPNIKE

Wow6432Node\Microsoft\Tracing
Mon Apr 18 16:31:07 2016    AppInstall_RASAPI32
Mon Apr 18 16:31:07 2016    AppInstall_RASMANCS
Mon Apr 18 15:58:59 2016    FrameworkService_RASAPI32
Mon Apr 18 15:58:59 2016    FrameworkService_RASMANCS
Mon Apr 18 15:26:55 2016    iexplore_RASAPI32
Mon Apr 18 15:26:55 2016    iexplore_RASMANCS
Mon Apr 18 15:45:05 2016    InstallAX_20_0_0_228_RASAPI32
Mon Apr 18 15:45:05 2016    InstallAX_20_0_0_228_RASMANCS
Mon Apr 18 15:45:13 2016    InstallPlugin_20_0_0_235_RASAPI32
Page 137

```
                              SOFTWARE OUTPUT.txt
Mon Apr 18 15:45:13 2016    InstallPlugin_20_0_0_235_RASMANCS
Wed Apr 20 12:57:32 2016    KIX32_RASAPI32

------------------------------------------
uninstall v.20140512
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT
hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

Wed Apr 20 14:59:18 2016 (UTC)
  Microsoft Silverlight v.5.1.41212.0

Wed Apr 20 13:37:19 2016 (UTC)
  Microsoft .NET Framework 4 Extended v.4.0.30319

Wed Apr 20 13:36:47 2016 (UTC)
  Microsoft .NET Framework 4 Client Profile v.4.0.30319

Wed Apr 20 13:20:08 2016 (UTC)
  McAfee Agent v.5.0.2.188

Tue Apr 19 20:00:03 2016 (UTC)
  Configuration Manager Client v.5.00.8239.1000

Mon Apr 18 16:02:28 2016 (UTC)
  McAfee Host Intrusion Prevention v.8.00.0600

Mon Apr 18 16:02:25 2016 (UTC)
  McAfee Host Intrusion Prevention v.8.00.0600

Mon Apr 18 16:00:10 2016 (UTC)
  Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219 v.10.0.40219

Mon Apr 18 16:00:06 2016 (UTC)
  Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000

Mon Apr 18 15:57:15 2016 (UTC)
  Cisco Systems VPN Client 5.0.07.0440 v.5.0.7

Mon Apr 18 15:45:54 2016 (UTC)
  WinZip 17.5 v.17.5.10480

Mon Apr 18 15:45:31 2016 (UTC)
  ActivClient x64 v.6.2

Mon Apr 18 15:43:15 2016 (UTC)
  Microsoft .NET Framework 4 Extended v.4.0.30319

Mon Apr 18 15:42:14 2016 (UTC)
  Microsoft .NET Framework 4 Client Profile v.4.0.30319

Mon Apr 18 15:37:43 2016 (UTC)
  DisplayLink Graphics v.7.9.665.0

Mon Apr 18 15:37:38 2016 (UTC)
  DisplayLink Core Software v.7.9.630.0

Mon Apr 18 15:30:46 2016 (UTC)
  Microsoft Policy Platform v.1.2.3602.0

Mon Apr 18 15:30:36 2016 (UTC)
```

Page 138

SOFTWARE OUTPUT.txt
   Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 v.12.0.21005
   Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 v.12.0.21005

Mon Apr 18 15:29:26 2016 (UTC)
   MPlayer2

Mon Apr 18 15:28:47 2016 (UTC)
   NVIDIA Control Panel 341.12 v.341.12
   NVIDIA Graphics Driver 341.12 v.341.12
   NVIDIA Install Application v.2.1002.154.1150

Mon Apr 18 15:27:42 2016 (UTC)
   Dell Touchpad v.8.1206.101.115

Mon Apr 18 15:26:54 2016 (UTC)
   DXM_Runtime

Wed Dec 30 13:27:50 2015 (UTC)
   Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50908

Wed Dec 30 09:57:45 2015 (UTC)
   Microsoft Office Office 64-bit Components 2010 v.14.0.7015.1000

Wed Dec 30 07:06:36 2015 (UTC)
   Microsoft Lync 2010 v.4.0.7577.4486

Wed Dec 30 00:26:49 2015 (UTC)
   Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010 v.14.0.7015.1000

Wed Dec 30 00:26:47 2015 (UTC)
   Microsoft Office Shared 64-bit MUI (English) 2010 v.14.0.7015.1000

Tue Dec 29 22:29:48 2015 (UTC)
   Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50903

Tue Dec 29 18:26:52 2015 (UTC)
   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161

Tue Dec 29 16:06:55 2015 (UTC)
   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148 v.9.0.30729.4148

Tue Jul 14 04:53:26 2009 (UTC)
   AddressBook
   Connection Manager
   DirectDrawEx
   Fontcore
   IE40
   IE4Data
   IE5BAKEX
   IEData
   MobileOptionPack
   SchedulingAgent
   WIC

Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Wed Apr 20 15:42:01 2016 (UTC)
   Mozilla Firefox 45.0.2 (x86 en-US) v.45.0.2
   Mozilla Maintenance Service v.45.0.2.5941

Wed Apr 20 15:01:54 2016 (UTC)
   Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
   Security Update for Microsoft Publisher 2010 (KB2817478) 32-Bit Edition
                          Page 139

SOFTWARE OUTPUT.txt
Update for Microsoft Office 2010 (KB3114404) 32-Bit Edition
Security Update for Microsoft Office Excel 2010 (KB3114564) 32-Bit Edition
Update for Microsoft Office 2010 (KB2553140) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2965310) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB3085528) 32-Bit Edition
Update for Microsoft Office 2010 (KB3054873) 32-Bit Edition
Update for Microsoft Office 2010 (KB2597087) 32-Bit Edition
Update for Microsoft Office 2010 (KB2589386) 32-Bit Edition
Update for Microsoft Office 2010 (KB3054886) 32-Bit Edition
Security Update for Microsoft Visio 2010 (KB3114402) 32-Bit Edition
Update for Microsoft Office 2010 (KB2553388) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2920748) 32-Bit Edition
Update for Microsoft Office 2010 (KB3055047) 32-Bit Edition
Update for Microsoft Outlook 2010 (KB2760779) 32-Bit Edition
Update for Microsoft Office 2010 (KB2825640) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB3054848) 32-Bit Edition
Update for Microsoft Office 2010 (KB2883019) 32-Bit Edition
Update for Microsoft Office 2010 (KB2589298) 32-Bit Edition
Security Update for Microsoft Access 2010 (KB3101544) 32-Bit Edition
Security Update for Microsoft InfoPath 2010 (KB2878230) 32-Bit Edition
Definition Update for Microsoft Office 2010 (KB3114412) 32-Bit Edition
Update for Microsoft Outlook Social Connector 2010 (KB2553308) 32-Bit Edition
Update for Microsoft Filter Pack 2.0 (KB2881026) 32-Bit Edition
Update for Microsoft Office 2010 (KB2825635) 32-Bit Edition
Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition
Security Update for Microsoft PowerPoint 2010 (KB3114396) 32-Bit Edition
Update for Microsoft SharePoint Workspace 2010 (KB2760601) 32-Bit Edition

Wed Apr 20 15:01:53 2016 (UTC)
Microsoft Office Professional Plus 2010 v.14.0.7015.1000
Update for Microsoft Office 2010 (KB2589318) 32-Bit Edition
Update for Microsoft Office 2010 (KB2687275) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition
{90140000-0011-0000-0000-0000000FF1CE}_Office14.PROPLUS_{14984CC2-69CB-40F9-B3C2-5FF5
8163B8FA9}
Security Update for Microsoft Office 2010 (KB3114553) 32-Bit Edition
Update for Microsoft Office 2010 (KB2589375) 32-Bit Edition
Update for Microsoft Visio Viewer 2010 (KB2881021) 32-Bit Edition
Security Update for Microsoft Word 2010 (KB3114557) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2881029) 32-Bit Edition
Update for Microsoft Office 2010 (KB2791057) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2553313) 32-Bit Edition
Update for Microsoft InfoPath 2010 (KB2817369) 32-Bit Edition
Security Update for Microsoft OneNote 2010 (KB3054978) 32-Bit Edition
Update for Microsoft Office 2010 (KB2794737) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition
Update for Microsoft Office 2010 (KB3085512) 32-Bit Edition
Update for Microsoft Outlook 2010 (KB3101535) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition
Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Apr 20 14:56:14 2016 (UTC)
Adobe Flash Player 21 ActiveX v.21.0.0.182

Wed Apr 20 14:56:02 2016 (UTC)
Adobe Flash Player 21 NPAPI v.21.0.0.182

Wed Apr 20 13:37:03 2016 (UTC)
{8E34682C-8118-31F1-BC4C-98CD96675E1C2}.KB2162169
{8E34682C-8118-31F1-BC4C-98CD96675E1C2}.KB2416472
{8E34682C-8118-31F1-BC4C-98CD96675E1C2}.KB2468871
{8E34682C-8118-31F1-BC4C-98CD96675E1C2}.KB2478063

Page 140

```
                        SOFTWARE OUTPUT.txt
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2487367
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2533523
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2544514
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2572063
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2599651
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2600211
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2600217
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2604121
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2639327
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2656351
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2682543
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2736428
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2742595
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2836939
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2836939v2
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2836939v3
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2858302
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2858302v2
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2894842
Security Update for Microsoft .NET Framework 4 Extended (KB2894842v2) v.2
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2901110
{8E34682C-8118-31F1-BC4C-98CD9675E1C2}.KB2901110v2
Security Update for Microsoft .NET Framework 4 Extended (KB3037578) v.1
Security Update for Microsoft .NET Framework 4 Extended (KB3098778) v.1

Wed Apr 20 13:36:33 2016 (UTC)
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2160841
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2162169
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2446708
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2446708v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2468871
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2473228
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2478063
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2478663
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2514805
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2518870
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2533523
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2539636
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2544514
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2572063
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2572078
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2599651
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2600211
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2600217
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2604121
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2633870
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2639327
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2656351
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2656368
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2656368v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2656405
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2686827
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2698021
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2729449
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2732797
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2736428
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2737019
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2742595
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2789642
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2804576
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2832407
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2835393
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2836939
```

Page 141

```
                       SOFTWARE OUTPUT.txt
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2836939v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2836939v3
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2840628
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2840628v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2858302
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2858302v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2861188
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2894842
Security Update for Microsoft .NET Framework 4 Client Profile (KB2894842v2) v.2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2898842
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2898855
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2898855v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2901110
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2901110v2
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2931365
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2938780
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2938780v2
Security Update for Microsoft .NET Framework 4 Client Profile (KB2972106) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB2972215) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB2978125) v.1
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2979575
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB2979575v2
Security Update for Microsoft .NET Framework 4 Client Profile (KB3023221) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB3032662) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB3037578) v.1
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB3048074
{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}.KB3072309
Security Update for Microsoft .NET Framework 4 Client Profile (KB3074547) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB3097994) v.1
Security Update for Microsoft .NET Framework 4 Client Profile (KB3098778) v.1

Wed Apr 20 13:00:14 2016 (UTC)
  WebEx Training Manager for Firefox or Chrome v.29.13.40.10011

Wed Apr 20 12:59:59 2016 (UTC)
  Cisco WebEx Meeting Center for Firefox or Chrome v.29.13.41.10011

Wed Apr 20 12:59:43 2016 (UTC)
  WebEx Event Manager for Firefox or Chrome v.29.13.41.10011

Wed Apr 20 12:59:26 2016 (UTC)
  Google Chrome v.66.56.118

Tue Apr 19 20:55:59 2016 (UTC)
  GlobalSubmit Review 2014 v.8.2.2

Tue Apr 19 20:52:00 2016 (UTC)
  Google Update Helper v.1.3.29.5

Tue Apr 19 20:41:20 2016 (UTC)
  Cisco Jabber v.10.5.0.37889

Tue Apr 19 20:40:20 2016 (UTC)
  Cisco IP Communicator v.8.6.3.0

Mon Apr 18 16:27:08 2016 (UTC)
  Adobe Refresh Manager v.1.8.0

Mon Apr 18 16:00:10 2016 (UTC)
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063
```

Page 142

SOFTWARE OUTPUT.txt

Mon Apr 18 16:00:05 2016 (UTC)
  Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219 v.10.0.40219
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063

Mon Apr 18 16:00:02 2016 (UTC)
  Microsoft Visual C++ 2005 Redistributable v.8.0.61001

Mon Apr 18 15:58:41 2016 (UTC)
  McAfee VirusScan Enterprise v.8.8.04001

Mon Apr 18 15:57:46 2016 (UTC)
  Check Point Endpoint Security - Full Disk Encryption v.7.5.100.25

Mon Apr 18 15:56:59 2016 (UTC)
  {5FDC06BF-3D3D-4367-8FFB-4FAFCB61972D}

Mon Apr 18 15:56:55 2016 (UTC)
  Cisco AnyConnect Start Before Login Module v.3.1.05160

Mon Apr 18 15:56:54 2016 (UTC)
  Cisco AnyConnect Diagnostics and Reporting Tool v.3.1.05160
  Cisco AnyConnect Secure Mobility Client v.3.1.05160

Mon Apr 18 15:56:52 2016 (UTC)
  Cisco AnyConnect Secure Mobility Client  v.3.1.05160

Mon Apr 18 15:56:15 2016 (UTC)
  WebEx Productivity Tools v.2.36.13053.10004

Mon Apr 18 15:54:47 2016 (UTC)
  WebEx Document Suite v.29.13.40.10011

Mon Apr 18 15:54:46 2016 (UTC)
  WebEx Support Manager for Internet Explorer v.29.13.40.10011

Mon Apr 18 15:54:44 2016 (UTC)
  WebEx Training Manager for Internet Explorer v.29.13.40.10011

Mon Apr 18 15:54:43 2016 (UTC)
  Network Recording Player v.29.13.40.10011

Mon Apr 18 15:54:42 2016 (UTC)
  Cisco WebEx Meeting Center for Internet Explorer v.29.13.41.10011

Mon Apr 18 15:54:40 2016 (UTC)
  WebEx Poll Questionnaire Editor v.29.13.30.10011

Mon Apr 18 15:54:39 2016 (UTC)
  WebEx Event Manager for Internet Explorer v.29.13.41.10011

Mon Apr 18 15:54:25 2016 (UTC)
  Java(TM) 6 Update 38 v.6.0.380

Mon Apr 18 15:54:19 2016 (UTC)
  SAFE Servlet v.7.05.00.219

Mon Apr 18 15:54:07 2016 (UTC)
  Java(TM) 6 Update 17 v.6.0.170

Page 143

SOFTWARE OUTPUT.txt

Mon Apr 18 15:53:53 2016 (UTC)
  Oracle JInitiator 1.3.1.26

Mon Apr 18 15:53:51 2016 (UTC)
  Oracle JInitiator 1.3.1.22

Mon Apr 18 15:53:48 2016 (UTC)
  Oracle Jinitiator 1.3.1.18

Mon Apr 18 15:53:38 2016 (UTC)
  Oracle JInitiator 1.3.1.13

Mon Apr 18 15:44:52 2016 (UTC)
  Adobe Acrobat X Pro v.10.1.16

Mon Apr 18 15:30:36 2016 (UTC)
  Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.21005 v.12.0.21005.1
  Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005 v.12.0.21005.1
  Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 v.12.0.21005

Mon Apr 18 15:30:35 2016 (UTC)
  Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 v.12.0.21005

Mon Apr 18 15:28:10 2016 (UTC)
  Realtek Audio COM Components v.1.0.2

Mon Apr 18 15:28:06 2016 (UTC)
  Realtek High Definition Audio Driver v.6.0.1.6049

Mon Apr 18 15:27:22 2016 (UTC)
  Intel(R) Processor Graphics v.10.18.14.4099

Mon Apr 18 15:26:55 2016 (UTC)
  Citrix online plug-in - web v.12.1.0.30

Wed Dec 30 12:25:03 2015 (UTC)
  EMC SourceOne Offline Access v.6.72.0017

Wed Dec 30 12:23:41 2015 (UTC)
  Citrix online plug-in (HDX) v.12.1.0.30

Wed Dec 30 12:23:40 2015 (UTC)
  Citrix online plug-in (DV) v.12.1.0.30

Wed Dec 30 12:23:38 2015 (UTC)
  Citrix online plug-in (USB) v.12.1.0.30

Wed Dec 30 12:23:31 2015 (UTC)
  Citrix online plug-in (Web) v.12.1.0.30

Wed Dec 30 12:23:18 2015 (UTC)
  Access Card Utility v.1.4.2

Wed Dec 30 12:20:19 2015 (UTC)
  eRoom 7 Client v.503.196

Wed Dec 30 10:06:57 2015 (UTC)
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
  Update for Microsoft Office 2010 (KB3085605) 32-Bit Edition
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Wed Dec 30 10:06:56 2015 (UTC)
  Microsoft Office Proof (English) 2010 v.14.0.7015.1000

Page 144

SOFTWARE OUTPUT.txt

Wed Dec 30 09:57:51 2015 (UTC)
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Security Update for Microsoft OneNote 2010 (KB3054978) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 09:57:50 2015 (UTC)
    Microsoft Office OneNote MUI (English) 2010 v.14.0.7015.1000

Wed Dec 30 09:57:46 2015 (UTC)
    Security Update for Microsoft Office 2010 (KB2553313) 32-Bit Edition
    Security Update for Microsoft OneNote 2010 (KB3054978) 32-Bit Edition
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Update for Microsoft Office 2010 (KB3054886) 32-Bit Edition
    Security Update for Microsoft InfoPath 2010 (KB2878230) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
    Update for Microsoft Filter Pack 2.0 (KB2881026) 32-Bit Edition
    Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition
    Update for Microsoft SharePoint Workspace 2010 (KB2760601) 32-Bit Edition

Wed Dec 30 09:55:57 2015 (UTC)
    Update for Microsoft Excel 2010 (KB2956084) 32-Bit Edition

Wed Dec 30 09:55:56 2015 (UTC)
    Microsoft Office Word MUI (English) 2010 v.14.0.7015.1000
    Security Update for Microsoft Word 2010 (KB2965313) 32-Bit Edition
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 09:55:53 2015 (UTC)
    Microsoft Office Outlook MUI (English) 2010 v.14.0.7015.1000
    Security Update for Microsoft Word 2010 (KB2965313) 32-Bit Edition
    Update for Microsoft Outlook 2010 (KB3101535) 32-Bit Edition
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 09:55:13 2015 (UTC)
    Microsoft Office Shared MUI (English) 2010 v.14.0.7015.1000
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Update for Microsoft Office 2010 (KB2553140) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
    Security Update for Microsoft Office 2010 (KB2956076) 32-Bit Edition
    Security Update for Microsoft Office 2010 (KB3085560) 32-Bit Edition

Wed Dec 30 08:44:57 2015 (UTC)
    Microsoft Office PowerPoint MUI (English) 2010 v.14.0.7015.1000
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Update for Microsoft Excel 2010 (KB2956084) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
    Security Update for Microsoft PowerPoint 2010 (KB2920812) 32-Bit Edition

Wed Dec 30 08:44:54 2015 (UTC)
    Microsoft Office Excel MUI (English) 2010 v.14.0.7015.1000
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
    Update for Microsoft Excel 2010 (KB2956084) 32-Bit Edition
    Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 08:42:55 2015 (UTC)
    Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition

Wed Dec 30 08:42:54 2015 (UTC)
    Microsoft Office Proof (Spanish) 2010 v.14.0.7015.1000
    Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
                                Page 145

SOFTWARE OUTPUT.txt
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 08:42:51 2015 (UTC)
  Microsoft Office Proof (French) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:26:49 2015 (UTC)
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Wed Dec 30 00:26:47 2015 (UTC)
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Wed Dec 30 00:26:28 2015 (UTC)
  Microsoft Office Publisher MUI (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:26:25 2015 (UTC)
  Microsoft Office Proofing (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:26:12 2015 (UTC)
  Microsoft Office Shared Setup Metadata MUI (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:26:06 2015 (UTC)
  Microsoft Office InfoPath MUI (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:26:02 2015 (UTC)
  Microsoft Office Groove MUI (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:25:55 2015 (UTC)
  Microsoft Office Access Setup Metadata MUI (English) 2010 v.14.0.7015.1000
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:25:53 2015 (UTC)
  Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition
  Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Wed Dec 30 00:25:52 2015 (UTC)
  Microsoft Office Access MUI (English) 2010 v.14.0.7015.1000

Tue Dec 29 22:29:24 2015 (UTC)
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573

Tue Dec 29 22:29:19 2015 (UTC)
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573

Tue Dec 29 22:29:18 2015 (UTC)
  {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757
Page 146

SOFTWARE OUTPUT.txt
{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173

Tue Dec 29 18:43:45 2015 (UTC)
  Microsoft Office Professional Plus 2010 v.14.0.7015.1000

Tue Dec 29 18:27:34 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 v.9.0.30729.6161

Tue Dec 29 16:08:46 2015 (UTC)
  Microsoft Office Live Meeting 2007 v.8.0.6362.91

Tue Dec 29 16:05:49 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148

Tue Jul 14 04:53:25 2009 (UTC)
  AddressBook
  Connection Manager
  DirectDrawEx
  Fontcore
  IE40
  IE4Data
  IE5BAKEX
  IEData
  MobileOptionPack
  SchedulingAgent
  WIC


------------------------------------------
urlzone v.20090526
(Software) URLZONE detection

Microsoft\Windows\CurrentVersion\Internet Settings\urlzone not found.
Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userinit.exe not found.
------------------------------------------
uac v.20130213
(Software) Get Select User Account Control (UAC) Values from
HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem

UAC Information
Microsoft\Windows\CurrentVersion\policies\system
LastWrite Time Wed Apr 20 15:41:10 2016 (UTC)

EnableLUA value = 1

User Account Control: Run all administrators in Admin Approval Mode
0 = Disabled
1 = Enabled (Default)

EnableVirtualization value = 1

User Account Control: Virtualize file and registry write failures to per-user
locations
0 = Disabled
1 = Enabled (Default)

FilterAdministratorToken value = 1

User Account Control: Admin Approval Mode for the built-in Administrator account
0 = Disabled (Default)
1 = Enabled

ConsentPromptBehaviorAdmin value = 4

Page 147

SOFTWARE OUTPUT.txt

User Account Control: Behavior of the elevation prompt for administrators in Admin
Approval Mode
0 = Elevate without prompting
1 = Prompt for credentials on the secure desktop
2 = Prompt for consent on the secure desktop
3 = Prompt for credentials
4 = Prompt for consent
5 = Prompt for consent for non-Windows binaries (Default)

ConsentPromptBehaviorUser value = 1

User Account Control: Behavior of the elevation prompt for standard users
0 = Automatically deny elevation requests
1 = Prompt for consent on the secure desktop
3 = Prompt for consent on the secure desktop (Default)

-----------------------------------------
virut v.20130425
(Software) Detect Virut artifacts

Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time Tue Apr 19 20:03:56 2016 (UTC)

UpdateHost value not found.

Also be sure to check the SYSTEM\ControlSet00n\Services\SharedAccess\
Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List key
for exceptions added to the firewall; use the fw_config.pl plugin.
-----------------------------------------
win_cv v.20090312
(Software) Get & display the contents of the Windows\CurrentVersion key

Microsoft\Windows\CurrentVersion
LastWrite Time Mon Apr 18 15:50:45 2016 (UTC)

    SM_GamesName : Games
    ProgramFilesPath : %ProgramFiles%
    DevicePath : %SystemRoot%\inf
    ProgramFilesDir : C:\Program Files
    ProgramW6432Dir : C:\Program Files
    MediaPathUnexpanded : %SystemRoot%\Media
    ProgramFilesDir (x86) : C:\Program Files (x86)
    CommonFilesDir : C:\Program Files\Common Files
    CommonW6432Dir : C:\Program Files\Common Files
    SM_ConfigureProgramsName : Set Program Access and Defaults
    CommonFilesDir (x86) : C:\Program Files (x86)\Common Files
-----------------------------------------
winbackup v.20120812
(Software) Get Windows Backup

Microsoft\Windows\CurrentVersion\WindowsBackup\ScheduleParams\TargetDevice not
found.

Microsoft\Windows\CurrentVersion\WindowsBackup\Status not found.
-----------------------------------------
winlogon v.20130425
(Software) Get values from the WinLogon key

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Wed Apr 20 15:40:55 2016 (UTC)
    LegalNoticeCaption =
    LegalNoticeText =

Page 148

SOFTWARE OUTPUT.txt

```
ReportBootOk = 1
AutoRestartShell = 1
CachedLogonsCount = 2
ForceUnlockLogon = 0
PowerdownAfterShutdown = 0
ShutdownWithoutLogon = 0
WinStationsDisabled = 0
DisableCAD = 1
scremoveoption = 0
AutoLogonCount = 0
SyncForegroundPolicy = 1
allocatecdroms = 0
allocatedasd = 2
allocatefloppies = 0
autoadminlogon = 0
screensavergraceperiod = 5
DebugServerCommand = no
PasswordExpiryWarning = 14
ShutdownFlags = 167
Background = 0 0 0
Shell = explorer.exe
GinaDLL = pssogina.dll
Userinit = C:\Windows\system32\userinit.exe,
PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
VMApplet = SystemPropertiesPerformance.exe /pagefile
```

Notify subkey not found.

```
Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
  DefaultDomainName =
  DefaultUserName =
  ReportBootOk = 1
  Shell = explorer.exe
  Userinit = userinit.exe
  PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
  VMApplet = SystemPropertiesPerformance.exe /pagefile
```

Notify subkey not found.

Analysis Tips: The UserInit and Shell values are executed when a user logs on.
The UserInit value should contain a reference to userinit.exe; the Shell value
should contain just 'explorer.exe'. Check TaskMan & System values, if found.

Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList not found.
-------------------------------------------
winnt_cv v.20080609
(Software) Get & display the contents of the Windows NT\CurrentVersion key

WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Wed Apr 20 15:40:50 2016 (UTC)

  CurrentVersion : 6.1
  CurrentBuild : 7601
  RegisteredOwner : User
  CurrentBuildNumber : 7601
  CSDBuildNumber : 1130
  SoftwareType : System
  InstallationType : Client
  SystemRoot : C:\WINDOWS
  EditionID : Enterprise
  PathName : C:\WINDOWS
```

Page 149

SOFTWARE OUTPUT.txt

```
CM_DSLID : PS1:PS100204
CSDVersion : Service Pack 1
CurrentType : Multiprocessor Free
ProductName : Windows 7 Enterprise
ProductId : 00392-918-5000002-85077
RegisteredOrganization : Food and Drug Administration
BuildLab : 7601.win7sp1_gdr.151230-0600
InstallDate : Mon Apr 18 15:34:20 2016 (UTC)
BuildGUID : 9e51ce71-e025-4254-abf6-98e1b53566ca
BuildLabEx : 7601.19110.amd64fre.win7sp1_gdr.151230-0600
    DigitalProductId : a4 00 00 00 03 00 00 00 30 30 33 39 32 2d 39 31 38 2d 35 30 30
30 30 30 32 2d 38 35 30 37 37 00 aa 00 00 00 58 31 35 2d 33 39 31 36 36 00 00 00 00
00 00 00 7d 29 d9 af 2c 54 91 7d d6 ec d2 33 11 d2 04 00 00 00 00 00 8c 64 82 56 05
bc 75 34 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71
58 00 77
    DigitalProductId4 : f8 04 00 00 04 00 00 00 30 00 30 00 33 00 39 00 32 00 2d 00 30
00 30 00 31 00 37 00 30 00 2d 00 39 00 31 00 38 00 2d 00 35 00 30 00 30 00 30 00 30
00 30 00 2d 00 30 00 33 00 2d 00 31 00 30 00 33 00 33 00 2d 00 37 00 36 00 30 00 31
00 2e 00 30 00 30 00 30 00 30 00 2d 00 33 00 36 00 33 00 32 00 30 00 31 00 35 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 61 00 65 00 32 00 65 00 65 00 35 00 30 00 39 00 2d 00 31 00 62 00 33 00 34
00 2d 00 34 00 31 00 63 00 30 00 2d 00 61 00 63 00 62 00 37 00 2d 00 36 00 64 00 34
00 36 00 35 00 30 00 31 00 36 00 38 00 39 00 31 00 35 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 45 00 6e 00 74 00 65 00 72 00 70 00 72 00 69 00 73 00 65 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 7d 29 d9 af 2c 54 91 7d d6 ec d2 33 11 d2 04 00 16 30 79 89 9a 23 90 06 b2
bc af b7 99 13 48 c1 64 df a0 89 12 76 df f2 08 15 b6 0f d6 dc e2 04 e8 14 2a 73 d9
98 74 01 f2 46 f9 b7 80 9c 16 8e ea 81 83 1c ec 7b 8f 47 9d e4 9b 3d 18 2f 41 5f 58
00 31 00 35 00 2d 00 33 00 39 00 31 00 36 00 36 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 56 00 6f 00 6c 00 75 00 6d 00 65 00 3a
00 47 00 56 00 4c 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 56 00 6f 00 6c 00 75 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Page 150

```
                           SOFTWARE OUTPUT.txt
-------------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Windows 7 Enterprise
CSDVersion  = Service Pack 1
InstallDate = Mon Apr 18 15:34:20 2016
-------------------------------------------
yahoo_lm v.20101219
(SOFTWARE) Yahoo Messenger parser

Yahoo not found.
-------------------------------------------
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe
WARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:
pssogina.dll
```

Page 151

SYSTEM OUTPUT.txt
ControlSet001\Control\Session Manager\AppCertDlls not found.
------------------------------------------
appcompatcache v.20140724
(System) Parse files from System hive Shim Cache

Signature: 0xbadc0fee
Win2K8R2/Win7, 64-bit
C:\WINDOWS\SysWOW64\regsvr32.exe
ModTime: Tue Jul 14 01:14:30 2009 Z
Executed

C:\Program Files\ActivIdentity\ActivClient\accrdsub.exe
ModTime: Wed Jun  3 21:36:22 2009 Z
Executed

C:\WINDOWS\splwow64.exe
ModTime: Sun Nov 21 03:24:16 2010 Z
Executed

C:\WINDOWS\TEMP\B6494415-6E89-4CF2-8694-AD96AB7332CE\dismhost.exe
ModTime: Fri May 30 08:07:49 2014 Z
Executed

C:\WINDOWS\system32\makecab.exe
ModTime: Tue Jul 14 01:39:16 2009 Z
Executed

C:\PROGRA~2\WebEx\PRODUC~1\ptSrv.exe
ModTime: Mon Oct 12 06:06:12 2015 Z
Executed

C:\WINDOWS\CCM\RemCtrl\SccmRdpSystem.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe
ModTime: Thu Apr 16 19:14:29 2015 Z
Executed

C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe
ModTime: Mon Nov  5 20:27:46 2012 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\shext.dll
ModTime: Thu Jan 16 00:08:00 2014 Z

C:\WINDOWS\system32\{F33C3B9B-72AF-418A-B3FD-560646F7CDA2}.bat
ModTime: Mon Apr 18 16:25:28 2016 Z

C:\WINDOWS\System32\spoolsv.exe
ModTime: Sun Nov 21 03:24:27 2010 Z
Executed

C:\Windows\SysWOW64\InstallShield\_ISDEL.EXE
ModTime: Wed Jun 10 21:48:31 2009 Z
Executed

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashUtil32_20_0_0_228_ActiveX.exe
ModTime: Mon Apr 18 15:45:05 2016 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\USMT\USMTPercentScan.exe
ModTime: Thu Dec 12 21:10:36 2013 Z

Page 1

SYSTEM OUTPUT.txt

Executed

C:\WINDOWS\SysWOW64\windowspowershell\v1.0\powershell.exe
ModTime: Tue Jul 14 01:39:20 2009 Z
Executed

C:\WINDOWS\SysWOW64\tasklist.exe
ModTime: Tue Jul 14 01:14:42 2009 Z
Executed

C:\Program Files (x86)\Mozilla Maintenance Service\update\updater.exe
ModTime: Wed Mar 16 01:47:52 2016 Z
Executed

C:\WINDOWS\system32\igfxHK.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
Executed

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\xlicons.exe
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\WINDOWS\SysNative\dism.exe
ModTime: Tue Jul 14 01:39:06 2009 Z

C:\WINDOWS\TEMP\InstallPlugin_20_0_0_235.exe
ModTime: Tue Dec  1 18:12:58 2015 Z
Executed

C:\WINDOWS\Installer\MSI1FF0.tmp
ModTime: Tue Apr 19 20:41:10 2016 Z
Executed

C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
ModTime: Sun Nov 21 03:24:52 2010 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2972106-x64.exe
ModTime: Thu Mar 10 21:02:27 2016 Z
Executed

C:\Program Files (x86)\Windows Media Player\wmplayer.exe
ModTime: Wed Apr 29 18:06:48 2015 Z
Executed

C:\ProgramData\Dell\drivers\multiplatform_bios_btrfstboot\applyconfig.bat
ModTime: Fri Sep 27 05:56:57 2013 Z

C:\WINDOWS\system32\reg.exe
ModTime: Tue Jul 14 01:14:30 2009 Z
Executed

c:\738a018c74a5cf8b8d5489dd\Setup.exe
ModTime: Wed May 28 11:34:26 2014 Z
Executed

C:\ProgramData\webex\WebEx\1530\WbxDLInst.exe
ModTime: Fri Sep 11 08:20:04 2015 Z
Executed

C:\WINDOWS\CCM\ccmeval.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

Page 2

SYSTEM OUTPUT.txt

C:\WINDOWS\SysWOW64\find.exe
ModTime: Tue Jul 14 01:14:20 2009 Z
Executed

C:\WINDOWS\UDI\IsTouchEnabled.exe
ModTime: Fri Jun  7 16:00:34 2013 Z
Executed

C:\Program Files\Microsoft Office\Office14\ONFILTER.DLL
ModTime: Fri Jun 28 03:09:56 2013 Z

C:\WINDOWS\SysWOW64\cscript.exe
ModTime: Sat Oct 12 01:15:48 2013 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
ModTime: Thu Mar 18 18:27:13 2010 Z
Executed

C:\WINDOWS\system32\unregmp2.exe
ModTime: Tue Jul 14 01:39:48 2009 Z
Executed

C:\Program Files (x86)\Pointsec\Pointsec for PC\P95tray.exe
ModTime: Tue Oct  8 22:56:21 2013 Z
Executed

C:\WINDOWS\Installer\MSICF6F.tmp
ModTime: Mon Apr 18 15:58:26 2016 Z
Executed

C:\WINDOWS\system32\lsm.exe
ModTime: Sun Nov 21 03:23:53 2010 Z
Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
ModTime: Thu Sep 24 15:40:41 2015 Z
Executed

C:\WINDOWS\Installer\MSICF81.tmp
ModTime: Mon Apr 18 15:58:26 2016 Z
Executed

D:\GlobalSubmitReview\GSReview2014\Sleep_xp.exe
ModTime: Fri Aug 15 00:59:00 2003 Z

C:\Program Files\Windows Mail\wab.exe
ModTime: Sun Nov 21 03:24:32 2010 Z
Executed

C:\Windows\SysWOW64\mf.dll
ModTime: Tue Feb  3 03:12:22 2015 Z

C:\Windows\SysWOW64\networkexplorer.dll
ModTime: Sun Nov 21 03:24:15 2010 Z

C:\_SMSTaskSequence\Packages\FDA000DB\JInit13126\Setup.exe
ModTime: Wed Sep  5 10:23:24 2001 Z
Executed

C:\Program Files (x86)\Mozilla Firefox\maintenanceservice_installer.exe
ModTime: Wed Mar 16 01:47:33 2016 Z
Executed

Page 3

SYSTEM OUTPUT.txt

```
C:\WINDOWS\SoftwareDistribution\Download\Install\silverlight_x64.exe
ModTime: Wed Jan 13 00:22:46 2016 Z
Executed

C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe
ModTime: Thu Apr 16 19:14:29 2015 Z
Executed

D:\GlobalSubmitReview\GSReview2014\SetACL.exe
ModTime: Wed Aug 13 01:58:36 2003 Z

C:\WINDOWS\system32\oobe\msoobe.exe
ModTime: Sun Nov 21 03:23:52 2010 Z
Executed

C:\WINDOWS\Installer\MSID252.tmp
ModTime: Wed Apr 20 14:58:45 2016 Z
Executed

C:\WINDOWS\TEMP\GLJ81EC.tmp
ModTime: Mon Apr 18 15:53:46 2016 Z
Executed

C:\WINDOWS\TEMP\{8DE20547-0501-4200-8194-993185C298F1}\ISBEW64.exe
ModTime: Mon Apr 18 15:57:38 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA002D5\OSD-ciscoanyconnectinstall.cmd
ModTime: Mon Nov 17 14:22:30 2014 Z

C:\Program Files
(x86)\Google\Update\Install\{261C1A12-8322-468D-AFC2-C80CEBE89959}\50.0.2661.75_chro
me_installer.exe
ModTime: Wed Apr 13 01:12:22 2016 Z
Executed

C:\Windows\SysWOW64\syncui.dll
ModTime: Sun Nov 21 03:25:09 2010 Z

C:\WINDOWS\system32\oobe\windeploy.exe
ModTime: Sun Nov 21 03:24:24 2010 Z
Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
ModTime: Thu Sep 24 12:40:42 2015 Z
Executed

C:\WINDOWS\SysWOW64\SetIEInstalledDate.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\WINDOWS\Installer\MSI77F1.tmp
ModTime: Mon Apr 18 15:56:58 2016 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\DAInstall.exe
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\WINDOWS\TEMP\{0ED4EB69-CA7B-4CB4-BF63-E5A8C663D778}\ISBEW64.exe
ModTime: Mon Apr 18 15:57:37 2016 Z
Executed
```

Page 4

SYSTEM OUTPUT.txt

C:\WINDOWS\System32\wsqmcons.exe
ModTime: Sun Nov 21 03:24:49 2010 Z
Executed

C:\Windows\SysWOW64\twext.dll
ModTime: Sun Nov 21 03:24:32 2010 Z

C:\WINDOWS\Installer\MSIC9B3.tmp
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA0007A\reg_win7.exe
ModTime: Tue Jul 14 01:39:29 2009 Z
Executed

C:\WINDOWS\system32\GfxUIEx.exe
ModTime: Thu Apr 16 19:14:49 2015 Z
Executed

C:\WINDOWS\system32\mcbuilder.exe
ModTime: Sun Nov 21 03:24:26 2010 Z
Executed

C:\WINDOWS\system32\igfxCUIService.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
Executed

C:\WINDOWS\system32\atbroker.exe
ModTime: Tue Jul 14 01:38:55 2009 Z
Executed

C:\WINDOWS\System32\mobsync.exe
ModTime: Sun Nov 21 03:24:51 2010 Z
Executed

C:\WINDOWS\SysWOW64\lodctr.exe
ModTime: Tue Jul 14 01:14:22 2009 Z
Executed

C:\WINDOWS\SysWOW64\wevtutil.exe
ModTime: Tue Jul 14 01:14:44 2009 Z
Executed

C:\WINDOWS\TEMP\mfe30C.tmp\cleanup.exe
ModTime: Wed Mar  9 14:53:55 2016 Z
Executed

C:\WINDOWS\ccmcache\6\Add_Admins.BAT
ModTime: Mon Jun 11 14:44:08 2012 Z

C:\Program Files (x86)\Common Files\McAfee\DATReputation\mcdatrep.exe
ModTime: Mon Jan 25 15:20:08 2016 Z
Executed

C:\Program Files (x86)\Google\Chrome\Application\50.0.2661.75\Installer\setup.exe
ModTime: Tue Apr 19 20:40:55 2016 Z
Executed

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe
ModTime: Wed Mar 16 01:47:32 2016 Z
Executed

Page 5

SYSTEM OUTPUT.txt

C:\Program Files
(x86)\Google\Update\Install\{BE30EE67-B767-4F79-8012-E65F13FDE1E2}\chrome_installer.
exe
ModTime: Wed Apr 20 12:59:16 2016 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\scan64.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\WINDOWS\system32\verclsid.exe
ModTime: Tue Jul 14 01:39:49 2009 Z
Executed

C:\WINDOWS\SysWOW64\xcopy.exe
ModTime: Tue Jul 14 01:14:50 2009 Z
Executed

C:\Program Files\Common Files\Deterministic Networks\Common Files\dneinst.exe
ModTime: Sun Nov 16 22:39:43 2008 Z
Executed

c:\ca4fad583f94fa5f60fa4c\Setup.exe
ModTime: Tue Feb 10 09:27:02 2015 Z
Executed

C:\Program Files (x86)\GUM2990.tmp\GoogleUpdate.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA00080\5.0.07.0440\Win7CVPN5007_.CMD
ModTime: Fri Aug 12 17:38:47 2011 Z

C:\WINDOWS\Installer\MSICBA5.tmp
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\WINDOWS\system32\mpnotify.exe
ModTime: Tue Jul 14 01:39:20 2009 Z
Executed

C:\WINDOWS\Installer\MSIA4E8.tmp
ModTime: Wed Apr 20 12:59:12 2016 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrotray.exe
ModTime: Thu Sep 24 15:41:25 2015 Z
Executed

C:\Program Files\NVIDIA Corporation\Display\nvxdsync.exe
ModTime: Tue Nov  4 01:04:32 2014 Z
Executed

C:\WINDOWS\system32\SearchIndexer.exe
ModTime: Wed May  4 05:19:28 2011 Z
Executed

C:\WINDOWS\system32\consent.exe
ModTime: Thu Jun 25 10:06:15 2015 Z
Executed

c:\b51da2a2e71e216407b922aa8c65\Setup.exe
ModTime: Thu Jul  3 11:16:58 2014 Z

Page 6

SYSTEM OUTPUT.txt

Executed

c:\19f4e73b9d7033c49693\install.exe
ModTime: Sat Dec 12 05:11:00 2015 Z
Executed

C:\Program Files (x86)\webex\Productivity Tools\ptoneclk.exe
ModTime: Mon Oct 12 06:06:12 2015 Z

C:\WINDOWS\Installer\MSI4BB7.tmp
ModTime: Tue Apr 19 20:41:21 2016 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Designer 9.0\FormDesigner.exe
ModTime: Fri Oct  8 20:10:48 2010 Z
Executed

C:\WINDOWS\ccmcache\4\kb943280_hklm_regfix.cmd
ModTime: Mon Jan 27 21:31:55 2014 Z

C:\WINDOWS\system32\winsat.exe
ModTime: Sun Nov 21 03:24:35 2010 Z
Executed

C:\windows\System32\mf.dll
ModTime: Tue Feb  3 03:31:01 2015 Z

C:\_SMSTaskSequence\Packages\PS10018C\Uninst.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll
ModTime: Tue Jun 25 09:11:24 2013 Z

C:\Program Files (x86)\Pointsec\Pointsec for PC\fde_da_ew.exe
ModTime: Tue Oct  8 22:56:23 2013 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\macmnsvc.exe
ModTime: Wed Sep 23 23:57:26 2015 Z
Executed

C:\Program Files\DellTPad\HidFind.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\WINDOWS\CCM\UpdateTrustedSites.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\_SMSTaskSequence\Packages\PS1002F3\setup_util_x64.exe
ModTime: Thu Jun 25 01:40:10 2015 Z
Executed

C:\WINDOWS\Installer\MSI25A2.tmp
ModTime: Mon Apr 18 15:59:54 2016 Z
Executed

C:\ProgramData\McAfee\Common
Framework\Current\EPOAGENT3000\Install\0409\FramePkg.exe
ModTime: Wed Apr 20 13:18:06 2016 Z
Executed

Page 7

SYSTEM OUTPUT.txt

C:\WINDOWS\Installer\MSIB784.tmp
ModTime: Mon Apr 18 15:57:15 2016 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat Elements\ContextMenu.dll
ModTime: Thu Sep 24 15:41:01 2015 Z

C:\WINDOWS\TEMP\mfe41FF.tmp\cleanup.exe
ModTime: Thu Jun 11 17:12:44 2015 Z
Executed

C:\ProgramData\McAfee\Common
Framework\Evaluation\VIRUSCAN8800\Patch\7\0000\setup.exe
ModTime: Mon Apr 18 15:59:39 2016 Z
Executed

C:\WINDOWS\TEMP\{C012EC36-0D1B-471A-BEF2-C2D5553393BF}\InstallFlashPlayer.exe
ModTime: Wed Apr 20 14:55:58 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA002C1\kb943280_hklm_regfix.cmd
ModTime: Mon Jan 27 21:31:55 2014 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\MSIPatchRegFix-AMD64.exe
ModTime: Thu Mar 10 21:00:19 2016 Z
Executed

C:\WINDOWS\SysWOW64\Prot_srv.exe
ModTime: Tue Oct  8 22:56:23 2013 Z
Executed

C:\WINDOWS\ccmsetup\vcredist_x64.exe
ModTime: Tue Apr 14 06:47:12 2015 Z
Executed

C:\_SMSTaskSequence\Packages\FDA000DB\jinit13118\Jinit13118.EXE
ModTime: Tue Feb  1 22:05:38 2005 Z
Executed

C:\WINDOWS\system32\wlrmdr.exe
ModTime: Tue Jul 14 01:39:55 2009 Z
Executed

c:\3cb5f26f2fc5f9d5c4e783d5be\Setup.exe
ModTime: Sun Jun 12 04:36:34 2011 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleUpdateComRegisterShell64.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
ModTime: Mon Apr 18 15:45:08 2016 Z
Executed

C:\PROGRA~2\WebEx\PRODUC~1\PTIM.exe
ModTime: Mon Oct 12 06:06:10 2015 Z
Executed

C:\WINDOWS\Explorer.EXE
ModTime: Sun Nov 21 03:24:11 2010 Z
Executed

Page 8

SYSTEM OUTPUT.txt

C:\WINDOWS\SysWOW64\reg.exe
ModTime: Tue Jul 14 01:14:30 2009 Z
Executed

C:\WINDOWS\TEMP\mfe30C.tmp\FrmInst.exe
ModTime: Wed Mar  9 14:53:55 2016 Z
Executed

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ModTime: Wed Apr 13 08:37:29 2016 Z
Executed

C:\Program Files\Microsoft Policy Platform\policyHost.exe
ModTime: Thu Aug  2 16:24:32 2012 Z
Executed

D:\GlobalSubmitReview\GSReview2014\Sleep_w7.exe
ModTime: Mon Aug 15 16:48:17 2011 Z

C:\Users\Abe-Arjun.Mallik\Documents\Misc\Downloads\iTunes6464Setup.exe
ModTime: Thu Oct 22 14:52:45 2015 Z

C:\WINDOWS\system32\runonce.exe
ModTime: Sun Nov 21 03:24:27 2010 Z
Executed

C:\WINDOWS\system32\tasklist.exe
ModTime: Tue Jul 14 01:39:47 2009 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework\v3.5\addinutil.exe
ModTime: Sun Nov 21 03:24:59 2010 Z
Executed

C:\Windows\System32\SearchFolder.dll
ModTime: Sun Nov 21 03:24:28 2010 Z

C:\WINDOWS\SysWOW64\msiexec.exe
ModTime: Mon Jun 15 21:42:49 2015 Z
Executed

C:\WINDOWS\system32\cscript.exe
ModTime: Sat Oct 12 01:15:48 2013 Z
Executed

C:\ProgramData\dell\drivers\multiplatform_bios_btrfstboot\x86_64\HAPI\hapint.exe
ModTime: Fri Sep 27 05:56:29 2013 Z
Executed

C:\Windows\system32\userinit.exe
ModTime: Sun Nov 21 03:24:28 2010 Z
Executed

C:\WINDOWS\TEMP\{D2B9C003-A3CD-44A0-9DE5-52FE986C03E5}\setlicense.exe
ModTime: Mon Apr 18 16:00:10 2016 Z
Executed

C:\WINDOWS\system32\PING.EXE
ModTime: Tue Jul 14 01:14:28 2009 Z

C:\Program Files (x86)\internet explorer\iexplore.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

Page 9

SYSTEM OUTPUT.txt

C:\Windows\Installer\{5FDC06BF-3D3D-4367-8FFB-4FAFCB61972D}\Icon09DB8A85.exe
ModTime: Mon Apr 18 15:56:59 2016 Z

C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
ModTime: Wed Nov 18 22:37:14 2015 Z
Executed

C:\Windows\System32\ieframe.dll
ModTime: Fri Nov  6 19:06:09 2015 Z

C:\_SMSTaskSequence\Packages\PS10018C\SetupVSE.Exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleCrashHandler64.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\Windows\SysWOW64\plugincp113122.cpl
ModTime: Tue Apr  5 08:38:20 2005 Z

C:\Windows\SysWOW64\plugincp113113.cpl
ModTime: Thu May  8 18:35:36 2003 Z

C:\_SMSTaskSequence\Packages\FDA0020E\Java_Inst.CMD
ModTime: Thu May  2 14:38:43 2013 Z

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler64.exe
ModTime: Tue Apr 19 20:47:28 2016 Z
Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\VACon64.exe
ModTime: Wed Mar 12 20:52:14 2014 Z
Executed

C:\WINDOWS\system32\wbem\wmiprvse.exe
ModTime: Sun Nov 21 03:24:15 2010 Z
Executed

C:\WINDOWS\SysWOW64\wbem\WMIC.exe
ModTime: Tue Jul 14 01:14:46 2009 Z
Executed

C:\Program Files (x86)\Cisco Systems\Cisco Jabber\wbxcOIEx.exe
ModTime: Thu Aug  7 23:05:36 2014 Z
Executed

C:\WINDOWS\SysWOW64\unlodctr.exe
ModTime: Sun Nov 21 03:24:01 2010 Z
Executed

C:\WINDOWS\TEMP\IE130DF.tmp\IE11-SUPPORT\IENRCORE.EXE
ModTime: Mon Oct 14 23:27:54 2013 Z
Executed

C:\Program Files (x86)\Microsoft Office\Office14\msohtmed.exe
ModTime: Tue Dec 18 04:47:24 2012 Z
Executed

Page 10

SYSTEM OUTPUT.txt

C:\WINDOWS\TEMP\vcredist_x86_2010.exe
ModTime: Fri Nov 22 19:59:18 2013 Z
Executed

C:\Windows\Installer\{3407ACEE-CEEE-46F3-BDBA-FF1830D4C42D}\_3ED46C0EFB35798DEEA279.
exe
ModTime: Wed Dec 30 12:23:18 2015 Z

C:\WINDOWS\Installer\MSICFA4.tmp
ModTime: Mon Apr 18 15:58:26 2016 Z
Executed

C:\Windows\System32\mssvp.dll
ModTime: Wed May  4 05:22:25 2011 Z

C:\WINDOWS\TEMP\maEF8C.tmp\x64\mfehidin.exe
ModTime: Wed Apr 20 13:19:10 2016 Z
Executed

C:\Program Files\DellTPad\HidMonitorSvc.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\WINDOWS\TEMP\InstallPlugin_21_0_0_182.exe
ModTime: Mon Mar  7 20:52:56 2016 Z
Executed

C:\WINDOWS\system32\DRIVERS\o2flash.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\WINDOWS\CCM\TsManager.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\Windows\System32\grpconv.exe
ModTime: Tue Jul 14 01:39:11 2009 Z
Executed

C:\WINDOWS\System32\taskkill.exe
ModTime: Tue Jul 14 01:39:47 2009 Z
Executed

C:\Users\ad_dcc_s.nchotu\AppData\Local\Temp\46EF.tmp\jabber-bootstrap.bat
ModTime: Tue Apr 19 20:41:20 2016 Z

C:\WINDOWS\CCM\TSMBootstrap.exe
ModTime: Fri May  8 04:59:59 2015 Z
Executed

C:\WINDOWS\system32\find.exe
ModTime: Tue Jul 14 01:39:10 2009 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler.exe
ModTime: Tue Apr 19 20:47:28 2016 Z
Executed

C:\WINDOWS\system32\net1.exe
ModTime: Sun Nov 21 03:24:07 2010 Z
Executed

Page 11

SYSTEM OUTPUT.txt
```
C:\Program Files (x86)\Cisco Systems\Cisco Jabber\CiscoJabber.exe
ModTime: Thu Aug  7 23:05:34 2014 Z

C:\_SMSTaskSequence\Packages\FDA000DB\jinit13122\data1.hdr
ModTime: Tue Apr  5 09:39:20 2005 Z

C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE
ModTime: Sat Oct 31 09:26:15 2015 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ngen.exe
ModTime: Thu Mar 18 17:16:28 2010 Z
Executed

C:\Windows\SysWOW64\PhotoMetadataHandler.dll
ModTime: Tue Jul 14 01:16:12 2009 Z

C:\ProgramData\webex\WebEx\1530\atasinst.exe
ModTime: Fri Sep 11 08:19:50 2015 Z
Executed

C:\_SMSTaskSequence\Packages\FDA002C1\reg_64.exe
ModTime: Tue Jul 14 01:39:30 2009 Z
Executed

C:\WINDOWS\SysWOW64\net1.exe
ModTime: Sun Nov 21 03:24:16 2010 Z
Executed

C:\_SMSTaskSequence\Packages\FDA002D5\certmgr.exe
ModTime: Tue Jan 30 01:07:56 2001 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\WINDOWS\WinSxS\amd64_microsoft-windows-ie-pdm_31bf3856ad364e35_8.0.7600.16385_non
e_6425238b793ee910\PDMSetup.exe
ModTime: Tue Jul 14 01:39:26 2009 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe
ModTime: Mon Jun 15 17:21:32 2015 Z
Executed

C:\WINDOWS\TEMP\mfe41FF.tmp\FrmInst.exe
ModTime: Thu Jun 11 17:12:44 2015 Z
Executed

C:\Program Files (x86)\McAfee\Host Intrusion
Prevention\vscore\HIP8_15_4_0\x64\mfehidin.exe
ModTime: Mon Jun 15 17:22:30 2015 Z
Executed

C:\WINDOWS\system32\wbem\WmiApSrv.exe
ModTime: Tue Jul 14 01:39:55 2009 Z
Executed

C:\Program Files (x86)\Windows Mail\WinMail.exe
ModTime: Tue Jul 14 01:14:45 2009 Z
Executed
```

Page 12

SYSTEM OUTPUT.txt

```
C:\_SMSTaskSequence\Packages\PS1002EF\osd_flash20inst_activex.cmd
ModTime: Wed Dec 16 19:32:40 2015 Z

C:\WINDOWS\SysWOW64\HOSTNAME.EXE
ModTime: Tue Jul 14 01:14:21 2009 Z
Executed

C:\WINDOWS\system32\wuauclt.exe
ModTime: Fri Nov 20 18:54:15 2015 Z
Executed

C:\Program Files\DisplayLink Core Software\DisplayLinkUserAgent.exe
ModTime: Thu Oct 22 20:56:30 2015 Z
Executed

C:\WINDOWS\system32\DrvInst.exe
ModTime: Tue Jul 14 01:39:07 2009 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ngen.exe
ModTime: Thu Mar 18 18:27:13 2010 Z
Executed

C:\Windows\System32\wpdshext.dll
ModTime: Thu Jan 29 03:19:34 2015 Z

C:\WINDOWS\system32\HOSTNAME.EXE
ModTime: Tue Jul 14 01:39:12 2009 Z
Executed

c:\4f7a8a6edc50d2483adc8a511abde9a6\Setup.exe
ModTime: Thu Jul  3 11:16:58 2014 Z
Executed

C:\_SMSTaskSequence\Packages\FDA000DB\install_all.CMD
ModTime: Fri Feb 25 19:04:56 2011 Z

C:\ProgramData\webex\WebEx\500\nbrplay.exe
ModTime: Fri Sep 11 08:19:58 2015 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\CR_71467.tmp\setup.exe
ModTime: Tue Apr 19 20:40:55 2016 Z
Executed

C:\WINDOWS\system32\mspaint.exe
ModTime: Tue Jul 14 01:39:24 2009 Z

C:\Program Files (x86)\Mozilla Firefox\firefox.exe
ModTime: Wed Mar 16 01:47:11 2016 Z
Executed

C:\Users\ad_dcc_s.nchotu\AppData\Local\Temp\E7EE.tmp\CopyBootstrap.bat
ModTime: Tue Apr 19 20:40:56 2016 Z

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\TargetPCLauncher.exe
ModTime: Thu Jul 31 04:37:44 2014 Z
Executed

c:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ServiceModelReg.exe
ModTime: Wed May 28 12:20:39 2014 Z
Executed
```

Page 13

```
                              SYSTEM OUTPUT.txt
C:\WINDOWS\Installer\MSIEF2F.tmp
ModTime: Tue Apr 19 20:40:58 2016 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateComRegisterShell64.exe
ModTime: Tue Apr 19 20:47:28 2016 Z
Executed

C:\Windows\SysWOW64\EhStorShell.dll
ModTime: Tue Jul 14 01:15:14 2009 Z

C:\_SMSTaskSequence\Packages\FDA000DB\jinit13122\Setup.exe
ModTime: Wed Sep  5 10:23:24 2001 Z
Executed

C:\WINDOWS\system32\CompatTelRunner.exe
ModTime: Fri Sep 18 19:22:39 2015 Z
Executed

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\accicons.exe
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe
ModTime: Wed Mar 16 01:47:44 2016 Z
Executed

C:\Program Files\Common Files\Microsoft Shared\Ink\InputPersonalization.exe
ModTime: Tue Jul 14 01:39:13 2009 Z
Executed

C:\WINDOWS\TEMP\vcredist_x64_2010.exe
ModTime: Fri Nov 22 19:59:18 2013 Z
Executed

C:\Windows\ccmcache\4\reg_64.exe
ModTime: Tue Jul 14 01:39:30 2009 Z
Executed

C:\WINDOWS\system32\DllHost.exe
ModTime: Tue Jul 14 01:39:06 2009 Z
Executed

C:\WINDOWS\TEMP\7976FD2E-D3DC-4D8E-B437-44CC363D4CE7\dismhost.exe
ModTime: Fri May 30 08:07:49 2014 Z
Executed

C:\WINDOWS\Installer\MSI7811.tmp
ModTime: Mon Apr 18 15:56:59 2016 Z
Executed

C:\PROGRA~2\McAfee\COMMON~1\McScanCheck.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\Program Files (x86)\Common Files\InstallShield\Engine\6\Intel 32\IKernel.exe
ModTime: Wed Sep  5 07:24:00 2001 Z
Executed

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\wordicon.exe
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\WINDOWS\Installer\MSI46C5.tmp
ModTime: Tue Apr 19 20:41:20 2016 Z
                              Page 14
```

SYSTEM OUTPUT.txt
Executed

C:\Program Files (x86)\GUME447.tmp\GoogleUpdate.exe
ModTime: Tue Apr 19 20:47:28 2016 Z
Executed

C:\Program Files\ActivIdentity\ActivClient\acevents.exe
ModTime: Wed Jun  3 21:38:32 2009 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleCrashHandler.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\Program Files (x86)\Citrix\ICA Client\wfcrun32.exe
ModTime: Tue Oct 12 22:28:26 2010 Z
Executed

C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ModTime: Tue Jul 14 01:14:24 2009 Z
Executed

C:\WINDOWS\TEMP\7DBA53D1-D0AF-46C3-8392-AE67C4DD47F9\dismhost.exe
ModTime: Fri May 30 08:07:49 2014 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\udaterui.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\Program Files\DisplayLink Core Software\dlua_630.exe
ModTime: Mon Apr 18 15:37:29 2016 Z
Executed

C:\WINDOWS\Installer\MSI49C3.tmp
ModTime: Tue Apr 19 20:41:21 2016 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\msipatchregfix-amd64.exe
ModTime: Thu Mar 10 21:02:43 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA0004E\Java_1.6_17.cmd
ModTime: Fri Jun 15 13:15:07 2012 Z

C:\WINDOWS\SysWOW64\rundll32.exe
ModTime: Tue Jul 14 01:14:31 2009 Z
Executed

C:\WINDOWS\sysnative\windowspowershell\v1.0\powershell.exe
ModTime: Tue Jul 14 01:39:20 2009 Z

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
ModTime: Thu Mar 20 22:50:31 2014 Z
Executed

C:\Windows\SysWOW64\shdocvw.dll
ModTime: Fri Jul 26 01:55:59 2013 Z

C:\WINDOWS\TEMP\{F2FCE38B-19E6-4FA0-A321-9765C6FE32D3}\InstallFlashPlayer.exe
ModTime: Mon Apr 18 15:45:11 2016 Z
Executed

Page 15

SYSTEM OUTPUT.txt

```
C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\pptico.exe
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files\FDA\Utils\WSAP.exe
ModTime: Tue Nov 15 15:04:38 2011 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\1\GUM209B.tmp\GoogleUpdateSetup.exe
ModTime: Fri Oct  2 20:17:22 2015 Z
Executed

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\outicon.exe
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files (x86)\Google\Chrome\Application\50.0.2661.75\Installer\chrmstp.exe
ModTime: Tue Apr 19 20:40:55 2016 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\McTray.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\Windows\System32\DeviceCenter.dll
ModTime: Sun Nov 21 03:23:51 2010 Z

C:\WINDOWS\ccmcache\2\ciscoanyconnect_copy_fdauseripsecprof.cmd
ModTime: Fri Apr 10 16:59:10 2015 Z

C:\WINDOWS\system32\StikyNot.exe
ModTime: Tue Jul 14 01:39:46 2009 Z

C:\Program Files\Microsoft Silverlight\5.1.41212.0\coregen.exe
ModTime: Sat Dec 12 03:42:25 2015 Z
Executed

C:\WINDOWS\system32\findstr.exe
ModTime: Sun Nov 21 03:24:08 2010 Z
Executed

C:\WINDOWS\CCM\SCNotification.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\WINDOWS\system32\_SMSOSDSetup\TsProgressUI.exe
ModTime: Sun Oct  4 22:04:59 2015 Z
Executed

C:\WINDOWS\system32\msiexec.exe
ModTime: Mon Jun 15 21:42:49 2015 Z
Executed

C:\WINDOWS\system32\taskmgr.exe
ModTime: Sun Nov 21 03:24:24 2010 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\UpdaterUI.exe
ModTime: Thu Sep 24 00:04:50 2015 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\shext.dll
ModTime: Thu Jan 16 00:08:00 2014 Z

C:\WINDOWS\Installer\MSIC5D8.tmp
```

Page 16

SYSTEM OUTPUT.txt
ModTime: Mon Apr 18 15:58:24 2016 Z
Executed

C:\WINDOWS\SYSTEM32\SETUPUGC.EXE
ModTime: Tue Jul 14 01:39:39 2009 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Xtras\AdobePDF\PrintINF64.exe
ModTime: Mon Oct 25 19:13:42 2010 Z
Executed

C:\WINDOWS\SysWOW64\net.exe
ModTime: Tue Jul 14 01:14:27 2009 Z
Executed

D:\Launch_PCRestore.exe
ModTime: Mon Nov 17 16:39:10 2014 Z

C:\Program Files\McAfee\Host Intrusion Prevention\ClientControl.exe
ModTime: Thu Jun 25 01:34:12 2015 Z
Executed

C:\WINDOWS\WinSxS\amd64_microsoft-windows-ie-gc-registeriepkeys_31bf3856ad364e35_11.
2.9600.16428_none_0a3fe92b38dd8c45\RegisterIEPKEYs.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\McScript_InUse.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe
ModTime: Tue Sep  1 18:13:59 2015 Z
Executed

C:\Program Files\DellTPad\Apntex.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\Windows\System32\EhStorShell.dll
ModTime: Tue Jul 14 01:40:36 2009 Z

C:\Program Files\NVIDIA Corporation\Display\nvtray.exe
ModTime: Tue Nov  4 01:04:32 2014 Z
Executed

C:\WINDOWS\system32\scrnsave.scr
ModTime: Tue Jul 14 01:38:53 2009 Z
Executed

C:\Windows\SysWOW64\FlashPlayerCPLApp.cpl
ModTime: Mon Apr 18 15:45:12 2016 Z

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\USMT\USMTRestore.exe
ModTime: Thu Jul 31 04:37:51 2014 Z

C:\Windows\SysWOW64\audiodev.dll
ModTime: Sun Nov 21 03:25:10 2010 Z

C:\WINDOWS\system32\OSDSETUPHOOK.EXE
ModTime: Sun Oct  4 22:04:59 2015 Z
Executed

Page 17

SYSTEM OUTPUT.txt

C:\WINDOWS\TEMP\_ISTMP1.DIR\_ISTMP0.DIR\uncrunch.exe
ModTime: Thu May  8 18:37:26 2003 Z
Executed

C:\_SMSTaskSequence\Packages\FDA00184\DigiSign.cmd
ModTime: Tue Sep  4 16:59:26 2012 Z

C:\Program Files (x86)\Citrix\ICA Client\concentr.exe
ModTime: Tue Oct 12 22:24:38 2010 Z
Executed

C:\WINDOWS\Installer\MSI5817.tmp
ModTime: Tue Apr 19 20:41:24 2016 Z
Executed

C:\WINDOWS\WinSxS\amd64_microsoft-windows-i..eoptionalcomponents_31bf3856ad364e35_11
.2.9600.16428_none_e410f56f6c4ee930\ConfigureIEOptionalComponents.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\naPrdMgr.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\WINDOWS\system32\svchost.exe
ModTime: Tue Jul 14 01:39:46 2009 Z
Executed

C:\Windows\system32\PrintIsolationHost.exe
ModTime: Tue Jul 14 01:39:27 2009 Z
Executed

C:\DMTFiles\CDMReport.exe
ModTime: Thu May 22 21:40:08 2014 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\CDM_Files\CDMUpdate_X64.exe
ModTime: Thu May 22 21:21:39 2014 Z
Executed

C:\WINDOWS\system32\Wat\WatAdminSvc.exe
ModTime: Tue Dec 29 20:46:10 2015 Z
Executed

C:\WINDOWS\Installer\MSICD1D.tmp
ModTime: Mon Apr 18 15:58:26 2016 Z
Executed

C:\WINDOWS\Installer\MSIA80.tmp
ModTime: Mon Apr 18 15:58:41 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA000C7\Adobe Acrobat X\Setup.exe
ModTime: Tue Nov  2 13:32:10 2010 Z
Executed

C:\Program Files\Internet Explorer\iexplore.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\progra~2\java\jre-1.6.38\bin\javaw.exe
ModTime: Mon Apr 18 15:54:25 2016 Z

Page 18

SYSTEM OUTPUT.txt
Executed

C:\WINDOWS\system32\wevtutil.exe
ModTime: Tue Jul 14 01:14:44 2009 Z
Executed

C:\Program Files (x86)\Java\jre6\bin\unpack200.exe
ModTime: Mon Apr 18 15:54:07 2016 Z
Executed

D:\Launch_PCBackup.exe
ModTime: Mon Nov 17 16:38:16 2014 Z

C:\WINDOWS\system32\schtasks.exe
ModTime: Sun Nov 21 03:24:26 2010 Z
Executed

C:\Windows\System32\networkexplorer.dll
ModTime: Sun Nov 21 03:24:02 2010 Z

C:\WINDOWS\WinSxS\amd64_microsoft-windows-i..-setieinstalleddate_31bf3856ad364e35_11
.2.9600.16428_none_eace14b8d6178cca\SetIEInstalledDate.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\WINDOWS\SysWOW64\wbem\mofcomp.exe
ModTime: Tue Jul 14 01:14:24 2009 Z
Executed

C:\WINDOWS\SysWOW64\RegisterIEPKEYS.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\WINDOWS\system32\lsass.exe
ModTime: Tue Oct 20 01:04:53 2015 Z
Executed

C:\ProgramData\webex\WebEx\1526\WbxDLInst.exe
ModTime: Fri Sep 11 08:20:04 2015 Z
Executed

C:\WINDOWS\system32\enstart64.exe
ModTime: Mon Apr 18 15:54:18 2016 Z
Executed

C:\WINDOWS\Installer\MSICB82.tmp
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\Windows\SysWOW64\ieframe.dll
ModTime: Fri Nov  6 18:47:35 2015 Z

C:\WINDOWS\TEMP\CR_08BB0.tmp\setup.exe
ModTime: Wed Apr 20 12:59:18 2016 Z
Executed

C:\WINDOWS\system32\mstsc.exe
ModTime: Tue Oct  1 23:31:09 2013 Z

C:\WINDOWS\CCM\OSDNetSettings.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

Page 19

```
                                SYSTEM OUTPUT.txt
C:\Program Files (x86)\Cisco Systems\VPN Client\vpnclient.exe
ModTime: Fri Mar  4 16:46:33 2011 Z
Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe
ModTime: Wed Mar 12 20:52:18 2014 Z
Executed

C:\_SMSTaskSequence\Packages\FDA00171\dotNetFx40_Full_setup.exe
ModTime: Thu Jun  7 18:52:52 2012 Z
Executed

C:\WINDOWS\CCM\RemCtrl\CmRcService.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe
ModTime: Thu Mar 18 17:16:28 2010 Z
Executed

C:\WINDOWS\Installer\MSIF9B1.tmp
ModTime: Wed Apr 20 14:58:56 2016 Z
Executed

C:\Windows\SysWOW64\InstallShield\setup.exe
ModTime: Wed Jun 10 21:48:32 2009 Z
Executed

C:\Program Files (x86)\EMC SourceOne\Offline Access\ExOAAgent.exe
ModTime: Sun Sep 18 18:29:01 2011 Z
Executed

C:\WINDOWS\CCM\Ccm32BitLauncher.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\_SMSTaskSequence\Packages\FDA0020E\jre-6u38-windows-i586.exe
ModTime: Wed Mar 27 15:14:35 2013 Z
Executed

C:\WINDOWS\Installer\MSI728D.tmp
ModTime: Mon Apr 18 15:56:57 2016 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\AcroDist.exe
ModTime: Thu Sep 24 15:41:29 2015 Z
Executed

C:\WINDOWS\SysWOW64\runonce.exe
ModTime: Sun Nov 21 03:23:53 2010 Z
Executed

C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
ModTime: Tue Jul 14 01:14:24 2009 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\masvc.exe
ModTime: Wed Sep 23 23:57:06 2015 Z
Executed

C:\WINDOWS\system32\xpsrchvw.exe
ModTime: Tue Jul 14 01:39:59 2009 Z
```

Page 20

```
                              SYSTEM OUTPUT.txt
C:\Program Files (x86)\Citrix\GoToMeeting\1189\G2MInstaller.exe
ModTime: Tue Apr 19 20:40:39 2016 Z
Executed

C:\Program Files\WinZip\WzPreviewer64.exe
ModTime: Mon Apr 29 21:50:00 2013 Z
Executed

C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\TabTip32.exe
ModTime: Tue Sep  1 17:52:16 2015 Z
Executed

C:\Program Files (x86)\Java\jre6\zipper.exe
ModTime: Sun Oct 11 09:02:28 2009 Z
Executed

C:\WINDOWS\system32\LogonUI.exe
ModTime: Sun Nov 21 03:24:09 2010 Z
Executed

C:\Program Files (x86)\eRoom 7\ERClient7.exe
ModTime: Tue Aug 23 07:44:32 2011 Z
Executed

C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe
ModTime: Thu Apr 16 19:14:29 2015 Z
Executed

C:\_SMSTaskSequence\Packages\PS1002F4\IE11-Windows6.1-x64-en-us.exe
ModTime: Thu Oct  9 19:38:41 2014 Z
Executed

D:\ChromeSetup (1).exe
ModTime: Fri Oct  2 20:17:22 2015 Z

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
ModTime: Thu Mar 18 17:16:28 2010 Z
Executed

C:\WINDOWS\SYSTEM32\cmd.exe
ModTime: Sun Nov 21 03:23:55 2010 Z
Executed

C:\WINDOWS\system32\Dwm.exe
ModTime: Tue Jul 14 01:39:08 2009 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\mcshield.exe
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\WINDOWS\TEMP\{05FCBA67-6D54-49E4-9761-BECFDF93372C}\InstallFlashPlayer.exe
ModTime: Wed Apr 20 14:56:07 2016 Z
Executed

C:\WINDOWS\TEMP\{AF27EDE3-3E6E-4DCB-A335-9603668E26D3}\InstallFlashPlayer.exe
ModTime: Mon Apr 18 15:45:03 2016 Z
Executed

C:\WINDOWS\system32\igfxTray.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
Executed
```

Page 21

SYSTEM OUTPUT.txt

C:\_SMSTaskSequence\Packages\PS1002D8\multiplatform_bios_btrfstboot.exe
ModTime: Thu Nov 19 19:42:52 2015 Z
Executed

C:\WINDOWS\System32\msdtc.exe
ModTime: Tue Jul 14 01:39:21 2009 Z
Executed

C:\Windows\SysWOW64\plugincpl13118.cpl
ModTime: Tue Mar  2 18:29:30 2004 Z

C:\Windows\system32\displayswitch.exe
ModTime: Tue Jul 14 01:39:06 2009 Z

C:\Windows\System32\dpapimig.exe
ModTime: Tue Jul 14 01:39:07 2009 Z
Executed

C:\WINDOWS\SysWOW64\DllHost.exe
ModTime: Tue Jul 14 01:14:18 2009 Z
Executed

C:\WINDOWS\ccmcache\1\ccmsetup.exe
ModTime: Sun Oct  4 22:04:59 2015 Z
Executed

C:\Program Files\DisplayLink Core Software\DisplayLinkManager.exe
ModTime: Thu Oct 22 20:56:28 2015 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3097994-x64.exe
ModTime: Thu Mar 10 20:16:37 2016 Z
Executed

C:\Program Files (x86)\Common Files\Check Point\UIFramework\cptray.exe
ModTime: Wed Jun  2 18:04:59 2010 Z
Executed

C:\WINDOWS\TEMP\{5CA23B93-6D15-48E6-9C39-18FFA4CD5B0C}\ISBEW64.exe
ModTime: Mon Apr 18 16:00:10 2016 Z
Executed

C:\_SMSTaskSequence\Packages\PS1001E9\CheckPoint_Install.CMD
ModTime: Thu Jan 22 15:24:32 2015 Z

C:\WINDOWS\system32\regsvr32.exe
ModTime: Tue Jul 14 01:39:29 2009 Z
Executed

C:\WINDOWS\ccmsetup\vc50727_x64.exe
ModTime: Tue Apr 14 06:47:12 2015 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrobat_sl.exe
ModTime: Thu Sep 24 15:40:41 2015 Z
Executed

C:\ProgramData\dell\drivers\multiplatform_bios_btrfstboot\x86_64\HAPI\dcmdev64.exe
ModTime: Fri Sep 27 05:56:25 2013 Z
Executed

C:\Program Files (x86)\WebEx\Document Suite\WbxDLInst.exe
ModTime: Fri Sep 11 08:20:04 2015 Z

Page 22

SYSTEM OUTPUT.txt

Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
ModTime: Thu Mar 18 20:47:22 2010 Z
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat Elements\ContextMenu64.dll
ModTime: Thu Sep 24 15:40:41 2015 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3074547-x64.exe
ModTime: Thu Mar 10 20:37:28 2016 Z
Executed

C:\WINDOWS\system32\wbem\unsecapp.exe
ModTime: Tue Jul 14 01:39:48 2009 Z
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\AudioTuningWizard.exe
ModTime: Tue Feb 12 18:14:26 2013 Z
Executed

C:\WINDOWS\TEMP\_ISTMP1.DIR\_INS5176._MP
ModTime: Mon Apr 18 15:53:28 2016 Z
Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\Temp\1882575568\AdobeARMHelper.exe
ModTime: Thu Sep 24 12:40:42 2015 Z
Executed

C:\WINDOWS\TEMP\InstallAX_21_0_0_182.exe
ModTime: Mon Mar  7 21:00:26 2016 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\ScriptSn.20160418115830.dll
ModTime: Mon Apr 18 15:58:25 2016 Z

C:\_SMSTaskSequence\Packages\PS1001D8\ciscoanyconnect_copy_fdauseripsecprof.cmd
ModTime: Fri Apr 10 16:59:10 2015 Z

C:\WINDOWS\TEMP\E3F58445-05BE-4AC6-91B5-6EB6F1A30CA8\dismhost.exe
ModTime: Fri May 30 08:07:49 2014 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\x64\mfehidin.exe
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\DAInstall.exe
ModTime: Mon Apr 18 15:58:24 2016 Z
Executed

C:\Windows\SysWOW64\mssvp.dll
ModTime: Wed May  4 04:32:02 2011 Z

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe
ModTime: Wed Mar 12 20:52:32 2014 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\MoveMouse.exe
ModTime: Fri Feb 17 02:36:22 2012 Z
Executed

C:\WINDOWS\system32\oobe\oobeldr.exe

Page 23

SYSTEM OUTPUT.txt
ModTime: Tue Jul 14 01:39:26 2009 Z
Executed

C:\WINDOWS\Installer\MSI2572.tmp
ModTime: Mon Apr 18 15:59:54 2016 Z
Executed

C:\WINDOWS\servicing\TrustedInstaller.exe
ModTime: Sun Nov 21 03:24:03 2010 Z
Executed

C:\Windows\System32\xcopy.exe
ModTime: Tue Jul 14 01:39:58 2009 Z
Executed

C:\_SMSTaskSequence\Packages\PS10018C\Uninstx64.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\WINDOWS\TEMP\vcredist_x86_2005.exe
ModTime: Thu Jun 14 15:05:20 2012 Z
Executed

C:\Windows\UDI\AppInstall.exe
ModTime: Thu Aug 30 17:06:36 2012 Z
Executed

C:\WINDOWS\Installer\MSIA60.tmp
ModTime: Mon Apr 18 15:58:41 2016 Z
Executed

C:\WINDOWS\system32\calc.exe
ModTime: Tue Jul 14 01:38:57 2009 Z

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\ManifestTool.exe
ModTime: Wed Mar 12 20:53:06 2014 Z
Executed

C:\WINDOWS\system32\getmac.exe
ModTime: Tue Jul 14 01:39:11 2009 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\msaconfig.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\ProgramData\dell\drivers\multiplatform_bios_btrfstboot\x86_64\HAPI\dchcfg64.exe
ModTime: Fri Sep 27 05:56:29 2013 Z
Executed

C:\WINDOWS\WinSxS\amd64_microsoft-windows-ie-pdm-configuration_31bf3856ad364e35_11.2
.9600.16428_none_32a601ad2b7a554f\PDMSetup.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\WINDOWS\SysWOW64\dism.exe
ModTime: Tue Jul 14 01:39:06 2009 Z
Executed

C:\WINDOWS\system32\atashost.exe
ModTime: Fri Sep 11 08:19:50 2015 Z

Page 24

SYSTEM OUTPUT.txt
C:\WINDOWS\WinSxS\x86_microsoft-windows-ie-gc-registeriepkeys_31bf3856ad364e35_11.2.
9600.16428_none_ae214da780801b0f\RegisterIEPKEYs.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\macompatsvc.exe
ModTime: Wed Sep 23 23:56:46 2015 Z
Executed

C:\WINDOWS\Installer\MSI66D0.tmp
ModTime: Mon Apr 18 15:56:54 2016 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3023221-x64.exe
ModTime: Thu Mar 10 20:44:31 2016 Z
Executed

C:\WINDOWS\system32\services.exe
ModTime: Mon Apr 13 03:28:33 2015 Z
Executed

D:\GoToMeeting Codec\g2m_codec.exe
ModTime: Thu Sep 12 18:35:04 2013 Z

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\communicatork9.exe
ModTime: Tue Feb 12 18:14:38 2013 Z
Executed

C:\Program Files\ActivIdentity\ActivClient\acsagent.exe
ModTime: Wed Jun  3 21:35:56 2009 Z
Executed

C:\WINDOWS\SYSTEM32\WISPTIS.EXE
ModTime: Sun Nov 21 03:25:10 2010 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VsTskMgr.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3032662-x64.exe
ModTime: Thu Mar 10 20:44:08 2016 Z
Executed

C:\WINDOWS\TEMP\Microsoft .NET Framework 4 Setup_4.0.30319\TMP2FFE.tmp.exe
ModTime: Thu Mar 18 23:32:37 2010 Z
Executed

C:\Program Files
(x86)\Google\Update\Install\{C2D88CF0-7ACE-487A-AFB9-09001DC35F2C}\GoogleUpdateSetup
.exe
ModTime: Wed Jan 20 17:58:00 2016 Z
Executed

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\Helper.exe
ModTime: Thu Jun 25 01:31:02 2015 Z
Executed

C:\WINDOWS\ccmsetup\ccmsetup.exe
ModTime: Sun Oct  4 22:04:59 2015 Z
Executed

C:\Users\ad_dcc_s.nchotu\AppData\Local\Temp\g2mA498.tmp\G2MInstHigh.exe
Page 25

SYSTEM OUTPUT.txt
ModTime: Tue Apr 19 20:40:39 2016 Z
Executed

C:\PROGRA~2\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
ModTime: Wed Sep  5 07:24:00 2001 Z
Executed

c:\dac6f6cbcef6992dde8507\Setup.exe
ModTime: Sun Jun 12 04:36:34 2011 Z
Executed

C:\WINDOWS\SysWOW64\PstartSr.exe
ModTime: Tue Oct  8 22:56:21 2013 Z
Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\VAInst64.exe
ModTime: Fri Mar  4 16:51:21 2011 Z
Executed

C:\Program Files (x86)\Java\jre6\bin\jqs.exe
ModTime: Mon Apr 18 15:54:07 2016 Z
Executed

C:\WINDOWS\CCM\CcmExec.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\WINDOWS\SYSTEM32\TAPIUNATTEND.EXE
ModTime: Tue Jul 14 01:39:47 2009 Z
Executed

C:\_SMSTaskSequence\Packages\FDA000DB\jinit1319\SETUP.EXE
ModTime: Wed Dec 17 16:30:30 1997 Z

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\1\GUM209B.tmp\GoogleUpdate.exe
ModTime: Tue Apr 19 20:40:05 2016 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
ModTime: Thu Mar 20 22:49:18 2014 Z
Executed

C:\Program Files\DellTPad\Apoint.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\WINDOWS\system32\compattel\DiagTrackRunner.exe
ModTime: Wed Jun  3 20:17:05 2015 Z
Executed

C:\WINDOWS\CCM\CcmRestart.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
ModTime: Sun Jan 10 02:34:23 2010 Z
Executed

C:\WINDOWS\system32\cmd.exe
ModTime: Sun Nov 21 03:24:03 2010 Z

C:\Program Files (x86)\Microsoft Silverlight\5.1.41212.0\coregen.exe
Page 26

SYSTEM OUTPUT.txt
ModTime: Sat Dec 12 03:12:28 2015 Z
Executed

C:\_SMSTaskSequence\Packages\FDA000DB\JInit13126\data1.hdr
ModTime: Tue May 16 09:50:54 2006 Z

C:\WINDOWS\SysWOW64\PING.EXE
ModTime: Tue Jul 14 01:14:28 2009 Z
Executed

C:\WINDOWS\system32\SearchProtocolHost.exe
ModTime: Wed May  4 05:19:28 2011 Z
Executed

C:\Program Files\McAfee\Host Intrusion Prevention\FireTray.exe
ModTime: Thu Jun 25 01:34:26 2015 Z
Executed

C:\WINDOWS\Setup\Scripts\SetupComplete.cmd
ModTime: Mon Apr 18 15:26:01 2016 Z

C:\Program Files\DellTPad\ApMsgFwd.exe
ModTime: Thu Apr 16 19:14:31 2015 Z
Executed

C:\WINDOWS\SysWOW64\sc.exe
ModTime: Tue Jul 14 01:14:35 2009 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\x64\DAInstall.exe
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\WINDOWS\system32\{C1D72DEE-FF54-4835-8F1C-DF56D09A95BE}.bat
ModTime: Mon Apr 18 16:25:28 2016 Z

C:\Windows\System32\cscui.dll
ModTime: Sun Nov 21 03:24:41 2010 Z

C:\WINDOWS\TEMP\Microsoft .NET Framework 4 Setup_4.0.30319\TMPCC93.tmp.exe
ModTime: Fri Mar 19 00:51:07 2010 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\McTray.exe
ModTime: Sat Jun 27 00:37:15 2015 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\CmdAgent.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

c:\922c3e20b4e138d3473990\Setup.exe
ModTime: Thu Feb  5 09:15:53 2015 Z
Executed

C:\Windows\SysWOW64\wpdshext.dll
ModTime: Thu Jan 29 03:02:08 2015 Z

C:\WINDOWS\TEMP\mfeC300.tmp\FrmInst.exe
ModTime: Tue Jun 25 20:08:00 2013 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\UpdateINI.exe
Page 27

```
                                         SYSTEM OUTPUT.txt
ModTime: Wed Nov 13 23:02:07 2013 Z
Executed

C:\WINDOWS\system32\net.exe
ModTime: Tue Jul 14 01:39:25 2009 Z
Executed

C:\WINDOWS\SysWOW64\cmd.exe
ModTime: Sun Nov 21 03:24:03 2010 Z
Executed

C:\Program Files\Common Files\System\wab32.dll
ModTime: Sat Oct  1 05:45:21 2011 Z

c:\821b926440bca534ebc99c\Setup.exe
ModTime: Fri Oct  2 09:16:10 2015 Z
Executed

C:\WINDOWS\System32\RegisterIEPKEYs.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\regasm.exe
ModTime: Thu Mar 20 22:50:32 2014 Z
Executed

C:\Program Files (x86)\Mozilla Firefox\updater.exe
ModTime: Wed Mar 16 01:47:52 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA00171\InstallDotNet4.cmd
ModTime: Fri Jan 31 17:58:36 2014 Z

C:\WINDOWS\system32\wusa.exe
ModTime: Sun Nov 21 03:24:08 2010 Z

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashUtil32_20_0_0_235_Plugin.exe
ModTime: Mon Apr 18 15:45:12 2016 Z
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\CDP\CDPinstall.exe
ModTime: Mon Jan 24 15:37:42 2011 Z
Executed

C:\_SMSTaskSequence\Packages\PS1002F3\McAfeeHIP_ClientSetup.exe
ModTime: Thu Aug 20 17:53:48 2015 Z
Executed

C:\WINDOWS\ccmsetup\cache\ccmsetup.exe
ModTime: Thu Jun 25 22:15:00 2015 Z
Executed

C:\WINDOWS\Installer\MSIB1F4.tmp
ModTime: Wed Apr 20 14:58:37 2016 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2972215-x64.exe
ModTime: Thu Mar 10 21:02:48 2016 Z
Executed

C:\_SMSTaskSequence\Packages\FDA0022E\winzip17_64bit.cmd
ModTime: Thu Jul 11 18:57:58 2013 Z
```

Page 28

SYSTEM OUTPUT.txt

```
D:\Firefox Setup 45.0.1.exe
ModTime: Mon Apr 11 20:35:30 2016 Z

C:\WINDOWS\system32\{A6D608F0-0BDE-491A-97AE-5C4B05D86E01}.bat
ModTime: Tue Apr 19 19:48:37 2016 Z

C:\Program Files (x86)\Java\jre6\bin\jusched.exe
ModTime: Mon Apr 18 15:54:07 2016 Z
Executed

C:\Program Files (x86)\GUMA62D.tmp\GoogleUpdate.exe
ModTime: Wed Apr 20 12:59:16 2016 Z
Executed

C:\_SMSTaskSequence\Packages\PS10022F\FramePkg_4.8.0.1938_FDSWV04575.exe
ModTime: Thu Jun 11 17:13:49 2015 Z
Executed

C:\Windows\System32\gameux.dll
ModTime: Fri Dec  7 13:15:31 2012 Z

C:\WINDOWS\WinSxS\x86_microsoft-windows-i..-setieinstalleddate_31bf3856ad364e35_11.2
.9600.16428_none_8eaf79351dba1b94\SetIEInstalledDate.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\_SMSTaskSequence\Packages\PS10018C\FramePkg_UPD.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\windows\System32\WUDFHost.exe
ModTime: Thu Jul 26 03:08:53 2012 Z
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleUpdateOnDemand.exe
ModTime: Tue Apr 19 20:40:07 2016 Z
Executed

C:\WINDOWS\SYSTEM32\IEUNATT.EXE
ModTime: Fri Nov  6 19:05:38 2015 Z
Executed

C:\WINDOWS\System32\sdclt.exe
ModTime: Sun Nov 21 03:25:06 2010 Z
Executed

C:\WINDOWS\system32\vssvc.exe
ModTime: Sun Nov 21 03:23:55 2010 Z
Executed

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\HipMgmt.exe
ModTime: Thu Jun 25 01:31:22 2015 Z
Executed

C:\Windows\system32\DeviceDisplayObjectProvider.exe
ModTime: Tue Jul 14 01:39:02 2009 Z
Executed

C:\_SMSTaskSequence\Packages\PS1002EF\osd_flash20inst_npapi.cmd
ModTime: Wed Dec 16 19:29:11 2015 Z

C:\WINDOWS\SysWOW64\netsh.exe
ModTime: Tue Jul 14 01:14:27 2009 Z
```

Page 29

SYSTEM OUTPUT.txt
Executed

C:\Program Files (x86)\Windows Media Player\wmpshare.exe
ModTime: Wed Apr 29 18:06:48 2015 Z
Executed

C:\Windows\UDI\OSDResults.exe
ModTime: Thu Aug 30 17:06:36 2012 Z
Executed

C:\WINDOWS\SYSTEM32\RUNDLL32.EXE
ModTime: Tue Jul 14 01:39:31 2009 Z
Executed

C:\Program Files (x86)\webex\Productivity Tools\ptonecli64.dll
ModTime: Mon Oct 12 06:06:12 2015 Z

C:\WINDOWS\System32\Wbem\WMIC.exe
ModTime: Tue Jul 14 01:14:46 2009 Z

C:\Program Files (x86)\Microsoft Lync\communicator.exe
ModTime: Thu Nov 12 22:00:18 2015 Z
Executed

C:\Windows\System32\fsquirt.exe
ModTime: Sun Nov 21 03:23:47 2010 Z
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe
ModTime: Thu Mar 18 21:23:04 2010 Z
Executed

C:\WINDOWS\Installer\MSIA4F.tmp
ModTime: Mon Apr 18 15:58:41 2016 Z
Executed

C:\WINDOWS\Installer\MSIE7D4.tmp
ModTime: Tue Apr 19 20:40:56 2016 Z
Executed

C:\Program Files (x86)\Java\jre6\bin\javaw.exe
ModTime: Mon Apr 18 15:54:07 2016 Z
Executed

C:\progra~2\java\jre-1.6.38\zipper.exe
ModTime: Wed Nov 14 09:18:29 2012 Z
Executed

C:\Program Files\Common Files\ActivIdentity\ac.sharedstore.exe
ModTime: Wed Jun  3 21:38:36 2009 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe
ModTime: Mon Jun 15 17:27:54 2015 Z
Executed

C:\DMTFiles\usmt\5\X64\loadstate.exe
ModTime: Thu Jul 26 01:12:12 2012 Z
Executed

C:\ProgramData\webex\WebEx\1525\WbxDLInst.exe
ModTime: Fri Sep 11 08:20:04 2015 Z
Executed

Page 30

SYSTEM OUTPUT.txt

C:\WINDOWS\system32\mfevtps.exe
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\Windows\System32\syncui.dll
ModTime: Sun Nov 21 03:24:51 2010 Z

C:\Windows\SysWOW64\plugincpl13126.cpl
ModTime: Tue May 16 08:49:59 2006 Z

C:\WINDOWS\TEMP\IE130DF.tmp\IE11-SUPPORT\IEXPLORE.EXE
ModTime: Mon Oct 14 22:48:14 2013 Z
Executed

C:\WINDOWS\system32\sppsvc.exe
ModTime: Sun Nov 21 03:23:56 2010 Z
Executed

C:\WINDOWS\TEMP\{5233B566-C0A7-499B-B831-47304F434D11}\InstallFlashPlayer.exe
ModTime: Wed Apr 20 14:55:56 2016 Z
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\CDP\certmgr.exe
ModTime: Fri Mar 18 18:12:34 2011 Z
Executed

C:\WINDOWS\CCM\TsProgressUI.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\WINDOWS\CCM\tsenv.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\Windows\System32\ntshrui.dll
ModTime: Wed Jan  4 10:44:20 2012 Z

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\regtlibv12.exe
ModTime: Thu Mar 18 18:27:13 2010 Z
Executed

C:\_SMSTaskSequence\WDPackage\fdascripts\ClearOfficeInitials\ClearOfficeInitials.cmd
ModTime: Fri Apr 11 11:24:09 2014 Z

C:\Windows\SysWOW64\acppage.dll
ModTime: Sun Nov 21 03:24:32 2010 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2978125-x64.exe
ModTime: Thu Mar 10 21:00:23 2016 Z
Executed

C:\WINDOWS\CCM\smsboot.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

C:\WINDOWS\system32\wbem\mofcomp.exe
ModTime: Tue Jul 14 01:39:20 2009 Z
Executed

C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
Executed

Page 31

SYSTEM OUTPUT.txt

C:\Program Files (x86)\Common Files\McAfee\SystemCore\DAInstall.exe
ModTime: Mon Apr 18 15:58:24 2016 Z
Executed

C:\WINDOWS\Installer\MSICD0D.tmp
ModTime: Mon Apr 18 15:58:26 2016 Z
Executed

C:\WINDOWS\SYSTEM32\MUIUNATTEND.EXE
ModTime: Tue Jul 14 01:39:24 2009 Z
Executed

C:\WINDOWS\Installer\MSIAB0.tmp
ModTime: Mon Apr 18 15:58:41 2016 Z
Executed

C:\Windows\System32\shdocvw.dll
ModTime: Fri Jul 26 02:24:56 2013 Z

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe
ModTime: Thu Mar 20 22:50:30 2014 Z
Executed

C:\Windows\SysWOW64\ntshrui.dll
ModTime: Wed Jan  4 08:58:41 2012 Z

C:\_SMSTaskSequence\Packages\FDA000DB\jInit13113\SETUP.EXE
ModTime: Wed Dec 17 15:30:30 1997 Z

C:\WINDOWS\system32\SearchFilterHost.exe
ModTime: Wed May  4 05:19:28 2011 Z
Executed

C:\WINDOWS\CCM\smsswd.exe
ModTime: Thu Jun 25 22:15:00 2015 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\mcupdate.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\_SMSTaskSequence\WDPackage\FDAscripts\ClearOfficeInitials\reg.exe
ModTime: Mon Apr 14 00:12:32 2008 Z
Executed

C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\1\7zS4ECB.tmp\setup.exe
ModTime: Wed Mar 16 01:50:15 2016 Z
Executed

C:\WINDOWS\TEMP\vcredist_x64_2005.exe
ModTime: Thu Jun 14 15:05:20 2012 Z
Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\cvpnd.exe
ModTime: Fri Mar  4 16:45:07 2011 Z
Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\InstallHelper.exe
ModTime: Wed Mar 12 20:52:08 2014 Z
Executed

Page 32

SYSTEM OUTPUT.txt
C:\_SMSTaskSequence\Packages\PS100169\DAT-Grab.bat
ModTime: Mon Feb 24 20:18:23 2014 Z

C:\WINDOWS\system32\rundll32.exe
ModTime: Tue Jul 14 01:14:31 2009 Z

C:\_SMSTaskSequence\Packages\PS1002F3\HF1059145\McAfeeHIP_ClientHotfix6_1059145.exe
ModTime: Wed Sep 16 20:04:00 2015 Z
Executed

C:\Program Files\Common Files\McAfee\SystemCore\EntVUtil.EXE
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3037578-x64.exe
ModTime: Thu Mar 10 20:45:30 2016 Z
Executed

C:\Program Files (x86)\Cisco Systems\Cisco Jabber\x64\wbxcOIEx64.exe
ModTime: Thu Jul 24 16:57:25 2014 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\maconfig.exe
ModTime: Wed Sep 23 23:56:54 2015 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\WINDOWS\WinSxS\x86_microsoft-windows-ie-pdm-configuration_31bf3856ad364e35_11.2.9
600.16428_none_d6876629731ce419\PDMSetup.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe
ModTime: Wed Mar 16 01:48:46 2016 Z
Executed

C:\Program Files (x86)\Microsoft Lync\UcMapi.exe
ModTime: Wed Sep 25 17:01:37 2013 Z
Executed

C:\_SMSTaskSequence\Packages\FDA00184\reg_w7.exe
ModTime: Mon Apr 14 00:12:32 2008 Z
Executed

c:\dc37314ae06ad4c7a127b2209f\Setup.exe
ModTime: Thu Feb  5 09:15:53 2015 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3098778-x64.exe
ModTime: Thu Mar 10 20:17:09 2016 Z
Executed

C:\PROGRA~1\COMMON~1\DETERM~1\DNE\dnes64x.exe
ModTime: Sun Nov 16 22:39:43 2008 Z
Executed

C:\WINDOWS\system32\taskeng.exe
ModTime: Sun Nov 21 03:24:27 2010 Z
Executed

Page 33

SYSTEM OUTPUT.txt

C:\_SMSTaskSequence\Packages\FDA0007A\IE_tabs_off.cmd
ModTime: Thu Nov 10 14:13:58 2011 Z

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
ModTime: Thu Mar 18 18:27:13 2010 Z
Executed

C:\dae0984bf92096849f7d22\Setup.exe
ModTime: Thu Mar 18 20:16:28 2010 Z
Executed

C:\WINDOWS\Installer\MSICAE4.tmp
ModTime: Mon Apr 18 15:58:25 2016 Z
Executed

C:\ProgramData\webex\WebEx\1526\WbxDLDrv.exe
ModTime: Fri Sep 11 08:20:04 2015 Z
Executed

C:\WINDOWS\SYSTEM32\DJOIN.EXE
ModTime: Sun Nov 21 03:24:09 2010 Z
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\mfeann.exe
ModTime: Thu Jan 16 00:08:00 2014 Z
Executed

C:\_SMSTaskSequence\Packages\PS10009B\OSDActivClientHotfix.cmd
ModTime: Fri Jan 31 01:19:04 2014 Z

C:\Windows\System32\PhotoMetadataHandler.dll
ModTime: Tue Jul 14 01:41:53 2009 Z

C:\WINDOWS\Installer\MSI458C.tmp
ModTime: Tue Apr 19 20:41:20 2016 Z
Executed

C:\WINDOWS\SysWOW64\wusa.exe
ModTime: Sun Nov 21 03:24:08 2010 Z
Executed

C:\WINDOWS\Installer\MSIF70C.tmp
ModTime: Mon Apr 18 15:58:36 2016 Z
Executed

C:\WINDOWS\system32\magnify.exe
ModTime: Tue Jul 14 01:39:16 2009 Z

C:\WINDOWS\system32\RAServer.exe
ModTime: Tue Jul 14 01:39:28 2009 Z
Executed

C:\WINDOWS\system32\nvvsvc.exe
ModTime: Tue Nov  4 01:04:27 2014 Z
Executed

C:\dae0984bf92096849f7d22\SetupUtility.exe
ModTime: Thu Mar 18 19:58:36 2010 Z
Executed

C:\_SMSTaskSequence\WDPackage\fdAscripts\CenterDesktopIcons-CM12\writeIcons.cmd
ModTime: Sun Feb  2 12:58:35 2014 Z

Page 34

SYSTEM OUTPUT.txt

C:\WINDOWS\system32\taskhost.exe
ModTime: Fri Nov 23 03:13:57 2012 Z
Executed

C:\ProgramData\webex\WebEx\1524\WbxDLInst.exe
ModTime: Fri Sep 11 08:20:04 2015 Z
Executed

C:\WINDOWS\ccmsetup\vcredist_x86.exe
ModTime: Tue Apr 14 06:47:08 2015 Z
Executed

c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe
ModTime: Wed May 28 11:50:18 2014 Z
Executed

C:\WINDOWS\system32\wermgr.exe
ModTime: Tue Jul 14 01:39:51 2009 Z
Executed

C:\Program Files\Microsoft Office\Office14\MAPISHELL.DLL
ModTime: Wed May 16 11:49:02 2012 Z

C:\_SMSTaskSequence\Packages\PS10001F\connect.bat
ModTime: Tue Jul 23 18:47:17 2013 Z

C:\WINDOWS\TEMP\{8D59EA37-C399-4770-85AB-352ACE11D6AA}\ISBEW64.exe
ModTime: Mon Aug 22 05:05:39 2011 Z
Executed

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\vscore\x64\mfehidin.exe
ModTime: Mon Jun 15 17:22:30 2015 Z
Executed

C:\WINDOWS\SysWOW64\atashost.exe
ModTime: Fri Sep 11 08:19:50 2015 Z
Executed

C:\WINDOWS\system32\lodctr.exe
ModTime: Tue Jul 14 01:39:15 2009 Z
Executed

C:\WINDOWS\WinSxS\x86_microsoft-windows-i..eoptionalcomponents_31bf3856ad364e35_11.2
.9600.16428_none_87f259ebb3f177fa\ConfigureIEOptionalComponents.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

C:\_SMSTaskSequence\Packages\FDA0004E\cacls.exe
ModTime: Mon Apr 14 09:42:14 2008 Z
Executed

C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe
ModTime: Thu Jun 25 01:34:18 2015 Z
Executed

C:\Program Files\McAfee\Host Intrusion Prevention\Helper.exe
ModTime: Thu Jun 25 01:34:08 2015 Z
Executed

C:\WINDOWS\CCM\OSDSetupWindows.exe
ModTime: Tue Apr 14 08:00:00 2015 Z
Executed

Page 35

```
                                SYSTEM OUTPUT.txt
C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\7z.exe
ModTime: Tue Feb  3 07:09:38 2009 Z
Executed


C:\Program Files\WinZip\WZSHLSTB.DLL
ModTime: Mon Apr 29 21:50:00 2013 Z


C:\WINDOWS\System32\SetIEInstalledDate.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed


C:\WINDOWS\Installer\MSI486B.tmp
ModTime: Tue Apr 19 20:41:20 2016 Z
Executed


C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\DMT_Files\USMT\rtconsole.exe
ModTime: Tue Jul 15 21:29:22 2008 Z
Executed


C:\WINDOWS\TEMP\2E44F53D-B930-40D5-B151-1C2641F2AA4D\dismhost.exe
ModTime: Fri May 30 08:07:49 2014 Z
Executed


C:\Program Files\Common Files\Microsoft Shared\OFFICE14\MSOXEV.DLL
ModTime: Mon Mar  1 10:18:08 2010 Z


C:\ProgramData\dell\drivers\multiplatform_bios_btrfstboot\x86_64\cctk.exe
ModTime: Fri Sep 27 06:19:56 2013 Z
Executed


D:\CitrixReceiver.exe
ModTime: Thu Oct 22 19:03:25 2015 Z


C:\Users\AD_DCC~1.NCH\AppData\Local\Temp\EnvWrapper.exe
ModTime: Thu Mar  6 18:31:23 2014 Z
Executed


C:\WINDOWS\system32\gpscript.exe
ModTime: Tue Jul 14 01:39:11 2009 Z
Executed


C:\Program Files\Windows Mail\WinMail.exe
ModTime: Tue Jul 14 01:39:53 2009 Z
Executed


C:\WINDOWS\SYSTEM32\OOBE\SETUPSQM.EXE
ModTime: Tue Jul 14 01:39:39 2009 Z
Executed


C:\Program Files (x86)\Cisco Systems\VPN Client\SetMTU.exe
ModTime: Fri Mar  4 16:45:35 2011 Z
Executed


C:\Program Files\WinZip\WINZIP64.EXE
ModTime: Mon Apr 29 21:50:00 2013 Z
Executed


C:\WINDOWS\TEMP\mfeC300.tmp\cleanup.exe
ModTime: Tue Jun 25 20:08:00 2013 Z
Executed


C:\WINDOWS\system32\igfxEM.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
```

Page 36

SYSTEM OUTPUT.txt

Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ServiceModelReg.exe
ModTime: Thu Mar 18 18:27:13 2010 Z
Executed

C:\WINDOWS\Installer\MSIFC6F.tmp
ModTime: Mon Apr 18 15:54:16 2016 Z
Executed

c:\cba99cb0f65e5bb18626ceb9\Setup.exe
ModTime: Tue Sep 29 14:25:22 2015 Z
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\ndp40-kb2894842-v2-x64.exe
ModTime: Wed Apr 15 03:30:29 2015 Z
Executed

C:\WINDOWS\TEMP\InstallAX_20_0_0_228.exe
ModTime: Sun Nov 22 00:42:20 2015 Z
Executed

C:\Program Files\WinZip\WZSHLS64.DLL
ModTime: Mon Apr 29 21:50:00 2013 Z

C:\Windows\Temp\{CAFECAFE-0013-0001-0122-ABCDEFABCDEF}\uncrunch.exe
ModTime: Tue Apr  5 08:38:40 2005 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\MfeServiceMgr.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\WINDOWS\system32\unlodctr.exe
ModTime: Tue Jul 14 01:39:48 2009 Z
Executed

C:\WINDOWS\system32\sc.exe
ModTime: Tue Jul 14 01:39:35 2009 Z
Executed

C:\Program Files\DisplayLink Core Software\cl_630.exe
ModTime: Mon Apr 18 15:37:28 2016 Z
Executed

C:\Windows\System32\ie4uinit.exe
ModTime: Tue Dec 29 19:21:35 2015 Z
Executed

c:\d88ce79680cc3b4427\Setup.exe
ModTime: Wed Jul 15 05:42:41 2015 Z
Executed

C:\WINDOWS\Installer\MSI21A6.tmp
ModTime: Tue Apr 19 20:41:11 2016 Z
Executed

C:\WINDOWS\system32\igfxext.exe
ModTime: Thu Apr 16 19:14:55 2015 Z
Executed

C:\Program Files (x86)\WebEx\Document Suite\atdoced.exe
ModTime: Fri Sep 11 08:19:50 2015 Z

Page 37

SYSTEM OUTPUT.txt

Executed

C:\WINDOWS\system32\SnippingTool.exe
ModTime: Tue Jul 14 01:39:41 2009 Z

C:\Users\ad_dcc_s.nchotu\Desktop\Launch_PCRestore.exe
ModTime: Mon Nov 17 16:39:10 2014 Z
Executed

C:\WINDOWS\system32\{86F549EB-A66B-4D6C-958D-CDDD66410751}.bat
ModTime: Mon Apr 18 16:25:28 2016 Z

C:\WINDOWS\WinSxS\x86_microsoft-windows-ie-pdm_31bf3856ad364e35_8.0.7601.17514_none_
0a379bcfbdcffb74\PDMSetup.exe
ModTime: Sun Nov 21 03:25:08 2010 Z
Executed

C:\PROGRA~2\WebEx\PRODUC~1\ptWbxONI.exe
ModTime: Mon Oct 12 06:06:12 2015 Z
Executed

C:\Windows\Temp\{61667728-A947-4C81-B55B-BC0DB504A47B}\Disk1\data1.hdr
ModTime: Mon Apr 18 16:02:56 2016 Z

C:\Program Files\Microsoft Office\Office14\MSOHEVI.DLL
ModTime: Thu Dec 13 17:48:59 2012 Z

C:\Windows\System32\prnfldr.dll
ModTime: Sun Nov 21 03:23:48 2010 Z

C:\_SMSTaskSequence\OSD\PS10018F\ccmsetup.exe
ModTime: Thu Jun 25 22:15:00 2015 Z
Executed

C:\WINDOWS\sysWOW64\wbem\wmiprvse.exe
ModTime: Sun Nov 21 03:24:27 2010 Z
Executed

C:\WINDOWS\system32\xcopy.exe
ModTime: Tue Jul 14 01:14:50 2009 Z

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\NGen.exe
ModTime: Thu Mar 20 22:49:19 2014 Z
Executed

C:\WINDOWS\system32\bcdedit.exe
ModTime: Sun Nov 21 03:24:22 2010 Z
Executed

C:\WINDOWS\Installer\MSI8AD8.tmp
ModTime: Mon Apr 18 15:57:03 2016 Z
Executed

C:\DMTFiles\usmt\5\X64\mighost.exe
ModTime: Wed Jul 25 23:23:59 2012 Z
Executed

C:\WINDOWS\Installer\MSIBD75.tmp
ModTime: Wed Apr 20 15:00:51 2016 Z
Executed

C:\WINDOWS\Installer\MSIAFD1.tmp
ModTime: Wed Apr 20 14:58:37 2016 Z

Page 38

SYSTEM OUTPUT.txt

Executed

c:\632d0829f292c3d51ff3c4ef\Setup.exe
ModTime: Fri Sep  5 16:26:44 2014 Z
Executed

C:\WINDOWS\TEMP\{B7D533EB-EC10-4B6C-94A4-818CBD64D2FA}\ISBEW64.exe
ModTime: Mon Apr 18 15:57:47 2016 Z
Executed

C:\WINDOWS\system32\netsh.exe
ModTime: Tue Jul 14 01:14:27 2009 Z
Executed

C:\WINDOWS\TEMP\{138211E2-283F-4ACA-A8B3-C76F016DDF90}\InstallFlashPlayer.exe
ModTime: Wed Apr 20 14:56:09 2016 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\policyupgrade.exe
ModTime: Thu Sep 24 00:06:22 2015 Z
Executed

C:\Windows\Temp\{CAFECAFE-0013-0001-0126-ABCDEFABCDEF}\uncrunch.exe
ModTime: Tue May 16 08:50:17 2006 Z
Executed

C:\progra~2\java\jre-1.6.38\bin\unpack200.exe
ModTime: Mon Apr 18 15:54:25 2016 Z
Executed

C:\Program Files (x86)\WebEx\Document Suite\ATKCall.exe
ModTime: Fri Sep 11 08:19:50 2015 Z
Executed

C:\Program Files (x86)\McAfee\Common Framework\frminst.exe
ModTime: Tue Feb 10 20:07:59 2015 Z
Executed

C:\WINDOWS\system32\wbem\WMIADAP.EXE
ModTime: Tue Jul 14 01:39:55 2009 Z
Executed

-------------------------------------------
auditfail v.20081212
(System) Get CrashOnAuditFail value

CrashOnAuditFail = 0
Feature is off; the system will not halt
-------------------------------------------
backuprestore v.20130904
(System) Gets the contents of the FilesNotToSnapshot, KeysNotToRestore, and
FilesNotToBackup keys

ControlSet001\Control\BackupRestore\FilesNotToSnapshot
LastWrite Time Tue Dec 29 15:55:11 2015 (UTC)
The listed directories/files are not backed up in Volume Shadow Copies

   WUA : %windir%\softwaredistribution\*.* /s
   OutlookOST : $UserProfile$\AppData\Local\Microsoft\Outlook\*.ost
   OutlookOAB : $UserProfile$\AppData\Local\Microsoft\Outlook\*.oab
   FVE : $AllVolumes$\System Volume
Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
   RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\*
                              Page 39

SYSTEM OUTPUT.txt
%ProgramData%\Microsoft\RAC\Outbound\* %ProgramData%\Microsoft\RAC\PublishedData\*
%ProgramData%\Microsoft\RAC\Temp\*
   OfficeODC :
$UserProfile$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\*.fsf
$UserProfile$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\*.fsd
$UserProfile$\Local Settings\Application Data\Office\14.0\OfficeFileCache\*.fsd
$UserProfile$\Local Settings\Application Data\Office\14.0\OfficeFileCache\*.fsf
$UserProfile$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEdit
Manager\*.fsf
$UserProfile$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEdit
Manager\*.fsd $UserProfile$\Local Settings\Application
Data\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\*.fsd $UserProfile$\Local
Settings\Application
Data\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\*.fsf

FilesNotToBackup key
ControlSet001\Control\BackupRestore\FilesNotToBackup
LastWrite Time Mon Apr 18 15:29:00 2016 (UTC)
Specifies the directories and files that backup applications should not backup or
restore

   Temporary Files : %TEMP%\* /s
   Power Management : \hiberfil.sys
   Memory Page File : \Pagefile.sys
   Offline Files Cache : C:\WINDOWS\CSC\* /s
   Netlogon : %SystemRoot%\netlogon.chg
   Internet Explorer : %UserProfile%\index.dat /s
   BITS_LOG : C:\WINDOWS\System32\Bits.log
   BITS_BAK : C:\WINDOWS\System32\Bits.bak
   WUA : %windir%\softwaredistribution\*.* /s
   WER : %ProgramData%\Microsoft\Windows\WER\* /s
   BITS_metadata : C:\ProgramData\Microsoft\Network\Downloader\*
   ETW : %SystemRoot%\system32\LogFiles\WMI\RtBackup\*.*
   Kernel Dumps : %systemroot%\Minidump\* /s %systemroot%\memory.dmp
   Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase
   VSS Default Provider : \System Volume
Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
   VSS Service DB : \System Volume
Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB
   FVE_Log : \System Volume Information\FVE.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}
   FVE_Wipe : \System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
   VSS Service Alternate DB : \System Volume
Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}ALT
   FVE_Control : \System Volume
Information\FVE.{e40ad34d-dae9-4bc7-95bd-b16218c10f72}.*
   MS Distributed Transaction Coordinator : C:\WINDOWS\system32\MSDtc\MSDTC.LOG
C:\WINDOWS\system32\MSDtc\trace\dtctrace.log
   RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\*
%ProgramData%\Microsoft\RAC\Outbound\* %ProgramData%\Microsoft\RAC\PublishedData\*
%ProgramData%\Microsoft\RAC\Temp\*

KeysNotToRestore key
ControlSet001\Control\BackupRestore\KeysNotToRestore
LastWrite Time Tue Jul 14 04:49:01 2009 (UTC)

Specifies the names of the registry subkeys and values that backup applications
should not restore

   Mount Manager : MountedDevices\
   MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\ASR\
   Session Manager : CurrentControlSet\Control\Session Manager\AllowProtectedRenames
   Pending Rename Operations : CurrentControlSet\Control\Session
Manager\PendingFileRenameOperations

Page 40

```
                              SYSTEM OUTPUT.txt
   Pending Rename Operations2 : CurrentControlSet\Control\Session
Manager\PendingFileRenameOperations2
-------------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = OCL0166192
TCP/IP Hostname = OCL0166192
-------------------------------------------
crashcontrol v.20131210
(System) Get crash control information

CrashDumpEnabled = 2 [Kernel memory dump]
DumpFile        = %SystemRoot%\MEMORY.DMP
MinidumpDir     = %SystemRoot%\Minidump
LogEvent        = 1
   Logs an event to the System Event Log (event ID = 1001, source = Save Dump)
-------------------------------------------
ddm v.20081129
(System) Get DDM data from Control Subkey

ControlSet001\Control\DDM not found.
-------------------------------------------
devclass v.20130630
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Tue Apr 19 19:48:25 2016 (UTC)
   Disk&Ven_&Prod_&Rev_8.07,B57D6A2F&0

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Device   : DISK&VEN_&PROD_&REV_8.07   SN: B57D6A2F&0
LastWrite: Tue Apr 19 19:48:27 2016 UTC


-------------------------------------------
disablelastaccess v.20090118
(System) Get NTFSDisableLastAccessUpdate value

NtfsDisableLastAccessUpdate
ControlSet001\Control\FileSystem
NtfsDisableLastAccessUpdate = 1
-------------------------------------------
dllsearch v.20100824
(System) Get crash control information

dllsearch v.20100824

CWDIllegalInDllSearch value not found.
-------------------------------------------
eventlog v.20090112
(System) Get EventLog configuration info


ActivIdentity \ Wed Dec 30 12:23:07 2015Z

Application \ Wed Apr 20 16:37:01 2016Z
   File             = %SystemRoot%\system32\winevt\Logs\Application.evtx
   DisplayNameFile  = %SystemRoot%\system32\wevtapi.dll
   MaxSize          = 20.00MB
```

Page 41

```
                                SYSTEM OUTPUT.txt
Retention        = 0 sec
AutoBackupLogFiles = 0


Cisco AnyConnect Diagnostics and Reporting Tool \ Mon Apr 18 15:56:54 2016Z
MaxSize          = 3.81MB
Retention        = 0 sec


Cisco AnyConnect Secure Mobility Client \ Mon Apr 18 15:56:52 2016Z
MaxSize          = 3.81MB
Retention        = 0 sec

HardwareEvents \ Tue Jul 14 04:49:01 2009Z
File             = %systemroot%\system32\winevt\logs\HardwareEvents.evtx
DisplayNameFile  = %SystemRoot%\system32\wecsvc.dll
MaxSize          = 20.00MB
Retention        = 0 sec

Internet Explorer \ Tue Jul 14 04:49:01 2009Z

Key Management Service \ Tue Jul 14 04:49:01 2009Z
MaxSize          = 20.00MB
Retention        = 0 sec

OAlerts \ Tue Dec 29 15:55:12 2015Z
DisplayNameFile  = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE14\OFFREL.DLL
MaxSize          = 128.00KB
Retention        = 0 sec

Pointsec \ Mon Apr 18 15:57:46 2016Z
File             = %SystemRoot%\System32\config\Pointsec.evt
MaxSize          = 512.00KB
Retention        = 7.00 days

Security \ Mon Apr 18 16:17:34 2016Z
File             = %SystemRoot%\System32\winevt\Logs\Security.evtx
DisplayNameFile  = %SystemRoot%\system32\wevtapi.dll
MaxSize          = 20.00MB
Retention        = 0 sec
WarningLevel     = 90

System \ Wed Apr 20 14:49:20 2016Z
File             = %SystemRoot%\system32\winevt\Logs\System.evtx
DisplayNameFile  = %SystemRoot%\system32\wevtapi.dll
MaxSize          = 20.00MB
Retention        = 0 sec

Windows PowerShell \ Tue Jul 14 04:49:01 2009Z
MaxSize          = 15.00MB
Retention        = 0 sec
AutoBackupLogFiles = 0

-------------------------------------
eventlogs v.20081219
(System) Gets Event Log settings from System hive

EventLog Configuration
ControlSet001\Services\Eventlog
LastWrite Time Mon Apr 18 15:57:46 2016 (UTC)
-------------------------------------
fw_config v.20080328
(System) Gets the Windows Firewall config from the System hive

Windows Firewall Configuration
                                Page 42
```

SYSTEM OUTPUT.txt
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
LastWrite Time Mon Apr 18 15:29:00 2016 (UTC)
        EnableFirewall -> 0
        DisableNotifications -> 0

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
LastWrite Time Mon Apr 18 15:29:00 2016 (UTC)
        EnableFirewall -> 0
        DisableNotifications -> 0


-------------------------------------------
hibernate v.20081216
(System) Check hibernation status

Error reading Heuristics value.
-------------------------------------------
ide v.20080418
(System) Get IDE device info from the System hive file

IDE
ControlSet001\Enum\IDE
LastWrite Time Wed Dec 30 04:39:26 2015 (UTC)

CdRomMsft_Virtual_CD/ROM_____1.0_____ [Wed Dec 30 14:08:03 2015]

DiskVirtual_HD_____1.1.0___ [Wed Dec 30 14:08:03 2015]
DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Wed Dec 30 13:52:01 2015 (UTC)
        DiskVirtual_HD_____1.1.0___,5&35dc7040&0&0.0.0
-------------------------------------------
imagedev v.20140104
(System)  --

imagedev
ControlSet001\Control\Class\{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}

Still Image Capture Devices
-------------------------------------------
kbdcrash v.20081212
(System) Checks to see if system is config to crash via keyboard

CrashOnCtrlScroll not set
-------------------------------------------
legacy v.20120524
(System) Lists LEGACY_* entries in Enum\Root key

Thu Apr 28 15:00:49 2016 (UTC)
  LEGACY_MFERKDET
  LEGACY_MFERKDET\0000 - McAfee Inc. mferkdet
Wed Apr 20 15:40:59 2016 (UTC)
  LEGACY_SRV\0000 - @%systemroot%\system32\srvsvc.dll,-102
  LEGACY_SRV2\0000 - @%systemroot%\system32\srvsvc.dll,-104
  LEGACY_SRVNET\0000 - srvnet
Wed Apr 20 15:40:58 2016 (UTC)
  LEGACY_BOWSER\0000 - @%systemroot%\system32\browser.dll,-102
  LEGACY_MRXSMB\0000 - @%systemroot%\system32\wkssvc.dll,-1002
  LEGACY_MRXSMB10\0000 - @%systemroot%\system32\wkssvc.dll,-1004
  LEGACY_MRXSMB20\0000 - @%systemroot%\system32\wkssvc.dll,-1006
Wed Apr 20 15:40:55 2016 (UTC)
  LEGACY_LUAFV\0000 - @%systemroot%\system32\drivers\luafv.sys,-100
Page 43

SYSTEM OUTPUT.txt

Wed Apr 20 15:40:47 2016 (UTC)
  LEGACY_DFSC\0000 - @%systemroot%\system32\drivers\dfsc.sys,-101
  LEGACY_MSFS\0000 - Msfs
  LEGACY_NETBIOS\0000 - NetBIOS Interface
  LEGACY_NPFS\0000 - Npfs
  LEGACY_RDBSS\0000 - @%systemroot%\system32\wkssvc.dll,-1000
Wed Apr 20 15:40:46 2016 (UTC)
  LEGACY_MUP\0000 - @%systemroot%\system32\drivers\mup.sys,-101
Wed Apr 20 15:40:45 2016 (UTC)
  LEGACY_ACSOCK\0000 - acsock
  LEGACY_AFD\0000 - @%systemroot%\system32\drivers\afd.sys,-1000
  LEGACY_BEEP\0000 - Beep
  LEGACY_CIPCCDP\0000 - Cisco IP Communicator driver for CDP
  LEGACY_CLFS\0000 - @%SystemRoot%\system32\clfs.sys,-100
  LEGACY_CNG\0000 - CNG
  LEGACY_CSC\0000 - @%systemroot%\system32\cscsvc.dll,-202
  LEGACY_CTXUSBM\0000 - Citrix USB Monitor Driver
  LEGACY_CVPNDRVA\0000 - Cisco Systems Inc. IPSec Driver
  LEGACY_DISCACHE\0000 - @%systemroot%\system32\drivers\discache.sys,-102
  LEGACY_DXGKRNL\0000 - LDDM Graphics Subsystem
  LEGACY_ENSTART64_\0000 - enstart64_
  LEGACY_FILEINFO\0000 - @%SystemRoot%\system32\drivers\fileinfo.sys,-100
  LEGACY_FLTMGR\0000 - @%SystemRoot%\system32\drivers\fltmgr.sys,-10001
  LEGACY_FS_REC\0000 - Fs_Rec
  LEGACY_FVEVOL\0000 - @%SystemRoot%\system32\drivers\fvevol.sys,-100
  LEGACY_HTTP\0000 - @%SystemRoot%\system32\drivers\http.sys,-1
  LEGACY_HWPOLICY\0000 - @%systemroot%\system32\drivers\hwpolicy.sys,-101
  LEGACY_KSECDD\0000 - KSecDD
  LEGACY_KSECPKG\0000 - KSecPkg
  LEGACY_LLTDIO\0000 - Link-Layer Topology Discovery Mapper I/O Driver
  LEGACY_MFEAACK\0000 - McAfee Inc. mfeaack
  LEGACY_MFEAPFK\0000 - McAfee Inc. mfeapfk
  LEGACY_MFEAVFK\0000 - McAfee Inc. mfeavfk
  LEGACY_MFEAVFK01\0000 - McAfee Inc.
  LEGACY_MFEFIREK\0000 - McAfee Inc. mfefirek
  LEGACY_MFEHIDK\0000 - McAfee Inc. mfehidk
  LEGACY_MFENLFK\0000 - McAfee NDIS Light Filter
  LEGACY_MFEWFPK\0000 - McAfee Inc. mfewfpk
  LEGACY_MOUNTMGR\0000 - @%SystemRoot%\system32\drivers\mountmgr.sys,-100
  LEGACY_MPSDRV\0000 - @%SystemRoot%\system32\FirewallAPI.dll,-23092
  LEGACY_MSISADRV\0000 - msisadrv
  LEGACY_NATIVEWIFIP\0000 - NativeWiFi Filter
  LEGACY_NDIS\0000 - @%SystemRoot%\system32\drivers\ndis.sys,-200
  LEGACY_NDISUIO\0000 - NDIS Usermode I/O Protocol
  LEGACY_NDPROXY\0000 - NDProxy
  LEGACY_NETBT\0000 - @%SystemRoot%\system32\drivers\netbt.sys,-2
  LEGACY_NSIPROXY\0000 - @%SystemRoot%\system32\drivers\nsiproxy.sys,-2
  LEGACY_NTFS\0000 - Ntfs
  LEGACY_NULL\0000 - Null
  LEGACY_PCW\0000 - Performance Counters for Windows Driver
  LEGACY_PEAUTH\0000 - PEAUTH
  LEGACY_PREPDRVR\0000 - SMS Process Event Driver
  LEGACY_PSCHED\0000 - @%SystemRoot%\System32\drivers\pacer.sys,-101
  LEGACY_RDPCDD\0000 - @%systemroot%\system32\DRIVERS\RDPCDD.sys,-100
  LEGACY_RDPDR\0000 - Terminal Server Device Redirector Driver
  LEGACY_RDPENCDD\0000 - @%systemroot%\system32\drivers\RDPENCDD.sys,-101
  LEGACY_RDPREFMP\0000 - @%systemroot%\system32\drivers\RdpRefMp.sys,-101
  LEGACY_RDPWD\0000 - RDP Winstation Driver
  LEGACY_RSPNDR\0000 - Link-Layer Topology Discovery Responder
  LEGACY_SPLDR\0000 - Security Processor Loader Driver
  LEGACY_TCPIP\0000 - @%SystemRoot%\system32\tcpipcfg.dll,-50003
  LEGACY_TCPIPREG\0000 - TCP/IP Registry Compatibility
  LEGACY_TDTCP\0000 - TDTCP

Page 44

SYSTEM OUTPUT.txt
```
    LEGACY_TDX\0000 - @%SystemRoot%\system32\tcpipcfg.dll,-50004
    LEGACY_TSSECSRV\0000 - @%SystemRoot%\System32\DRIVERS\tssecsrv.sys,-101
    LEGACY_VGASAVE\0000 - VgaSave
    LEGACY_VOLMGRX\0000 - @%SystemRoot%\system32\drivers\volmgrx.sys,-100
    LEGACY_VOLSNAP\0000 - Storage volumes
    LEGACY_VWIFIFLT\0000 - Virtual WiFi Filter Driver
    LEGACY_WANARPV6\0000 - @%systemroot%\system32\rascfg.dll,-32012
    LEGACY_WDF01000\0000 - @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000
    LEGACY_WFPLWF\0000 - WFP Lightweight Filter
    LEGACY_WUDFPF\0000 - @%SystemRoot%\system32\drivers\Wudfpf.sys,-1000
Wed Apr 20 14:49:08 2016 (UTC)
    LEGACY_MFEAACK01\0000 - McAfee Inc.
    LEGACY_MFEAVFK02\0000 - McAfee Inc.
    LEGACY_MFEHIDK01\0000 - McAfee Inc.
Wed Apr 20 13:19:22 2016 (UTC)
    LEGACY_MFEAACK01
Wed Apr 20 12:58:54 2016 (UTC)
    LEGACY_PREPDRVR
Tue Apr 19 20:40:21 2016 (UTC)
    LEGACY_CIPCCDP
Mon Apr 18 16:00:54 2016 (UTC)
    LEGACY_MFEAVFK02
Mon Apr 18 16:00:51 2016 (UTC)
    LEGACY_MFEFIREK
Mon Apr 18 16:00:41 2016 (UTC)
    LEGACY_MFEAACK
Mon Apr 18 16:00:28 2016 (UTC)
    LEGACY_MFEHIDK01
    LEGACY_MFENLFK
Mon Apr 18 15:58:32 2016 (UTC)
    LEGACY_MFEAPFK
    LEGACY_MFEAVFK01
Mon Apr 18 15:58:31 2016 (UTC)
    LEGACY_MFEAVFK
Mon Apr 18 15:58:30 2016 (UTC)
    LEGACY_MFEHIDK
    LEGACY_MFEWFPK
Mon Apr 18 15:57:15 2016 (UTC)
    LEGACY_CVPNDRVA
Mon Apr 18 15:56:52 2016 (UTC)
    LEGACY_ACSOCK
Mon Apr 18 15:54:18 2016 (UTC)
    LEGACY_ENSTART64_
Mon Apr 18 15:29:32 2016 (UTC)
    LEGACY_NATIVEWIFIP
    LEGACY_NDISUIO
Mon Apr 18 15:29:18 2016 (UTC)
    LEGACY_VOLSNAP
Mon Apr 18 15:29:01 2016 (UTC)
    LEGACY_RDPWD
    LEGACY_TDTCP
    LEGACY_TSSECSRV
Mon Apr 18 15:29:00 2016 (UTC)
    LEGACY_RDPDR
Mon Apr 18 15:28:04 2016 (UTC)
    LEGACY_VWIFIFLT
Mon Apr 18 15:27:22 2016 (UTC)
    LEGACY_DXGKRNL
Mon Apr 18 15:27:11 2016 (UTC)
    LEGACY_WUDFPF
Mon Apr 18 15:26:59 2016 (UTC)
    LEGACY_MRXDAV\0000 - @%systemroot%\system32\webclnt.dll,-104
    LEGACY_STORFLT\0000 - @%SystemRoot%\system32\vmstorfltres.dll,-1000
```
Page 45

```
                        SYSTEM OUTPUT.txt
    LEGACY_VMBUS\0000 - @%SystemRoot%\system32\vmbusres.dll,-1000
Mon Apr 18 15:26:58 2016 (UTC)
    LEGACY_ATAPI
    LEGACY_BOWSER
    LEGACY_COMPBATT
    LEGACY_HPSAMD
    LEGACY_HTTP
    LEGACY_ISAPNP
    LEGACY_LLTDIO
    LEGACY_LSI_SAS
    LEGACY_LSI_SCSI
    LEGACY_LUAFV
    LEGACY_MEGASR
    LEGACY_MPSDRV
    LEGACY_MRXSMB
    LEGACY_MRXSMB10
    LEGACY_MRXSMB20
    LEGACY_MSAHCI
    LEGACY_NVRAID
    LEGACY_PCIIDE
    LEGACY_PEAUTH
    LEGACY_RSPNDR
    LEGACY_SBP2PORT
    LEGACY_SRV
    LEGACY_SRV2
    LEGACY_SRVNET
    LEGACY_TCPIPREG
    LEGACY_WD
Mon Apr 18 15:26:57 2016 (UTC)
    LEGACY_ADP94XX
    LEGACY_ADPAHCI
    LEGACY_ADPU320
    LEGACY_ALIIDE
    LEGACY_AMDIDE
    LEGACY_AMDSATA
    LEGACY_AMDSBS
    LEGACY_ARC
    LEGACY_ARCSAS
    LEGACY_CMDIDE
    LEGACY_ELXSTOR
    LEGACY_IASTORV
    LEGACY_IIRSP
    LEGACY_INTELIDE
    LEGACY_LSI_FC
    LEGACY_LSI_SAS2
    LEGACY_MEGASAS
    LEGACY_MSDSM
    LEGACY_NFRD960
    LEGACY_NVSTOR
    LEGACY_QL2300
    LEGACY_QL40XX
    LEGACY_SISRAID2
    LEGACY_SISRAID4
    LEGACY_ST7007
    LEGACY_STEXSTOR
    LEGACY_STORVSC
    LEGACY_VIAIDE
    LEGACY_VSMRAID
Mon Apr 18 15:26:46 2016 (UTC)
    LEGACY_AFD
    LEGACY_BEEP
    LEGACY_CLFS
    LEGACY_CNG
                        Page 46
```

SYSTEM OUTPUT.txt

```
    LEGACY_CSC
    LEGACY_CTXUSBM
    LEGACY_DFSC
    LEGACY_DISCACHE
    LEGACY_FILEINFO
    LEGACY_FLTMGR
    LEGACY_FS_REC
    LEGACY_FVEVOL
    LEGACY_HWPOLICY
    LEGACY_KSECDD
    LEGACY_KSECPKG
    LEGACY_MSFS
    LEGACY_MUP
    LEGACY_NDIS
    LEGACY_NDPROXY
    LEGACY_NETBIOS
    LEGACY_NETBT
    LEGACY_NPFS
    LEGACY_NSIPROXY
    LEGACY_NTFS
    LEGACY_NULL
    LEGACY_PCW
    LEGACY_PSCHED
    LEGACY_RDBSS
    LEGACY_RDPCDD
    LEGACY_RDPENCDD
    LEGACY_RDPREFMP
    LEGACY_SPLDR
    LEGACY_STORFLT
    LEGACY_TCPIP
    LEGACY_TDX
    LEGACY_VGASAVE
    LEGACY_WANARPV6
    LEGACY_WFPLWF
Mon Apr 18 15:26:45 2016 (UTC)
    LEGACY_MOUNTMGR
    LEGACY_MSISADRV
    LEGACY_VMBUS
    LEGACY_VOLMGRX
    LEGACY_WDF01000
Wed Dec 30 14:08:12 2015 (UTC)
    LEGACY_SECDRV '
Wed Dec 30 14:01:34 2015 (UTC)
    LEGACY_MRXDAV
------------------------------------------
mountdev v.20130530
(System) Return contents of System hive MountedDevices key


MountedDevices
LastWrite time = Tue Apr 19 19:48:25 2016Z

\DosDevices\C:
    Drive Signature =  61 38 8d 01
\??\Volume{7221dbde-0587-11e6-9667-806e6f6e6963}
    Drive Signature =  61 38 8d 01

Device:
_??_USBSTOR#Disk&Ven_&Prod_&Rev_8.07#B57D6A2F&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8
b}
    \??\Volume{8fc79a65-0667-11e6-8233-34e6d733e6f7}
    \DosDevices\D:
```

Page 47

SYSTEM OUTPUT.txt
----------------------------------------
network v.20080324
(System) Gets info from System\Control\Network GUIDs

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}
Interface {033026B9-7329-415D-8068-DD988B393525}
LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
        Name                = Wireless Network Connection
        PnpInstanceID       =
PCI\VEN_8086&DEV_095A&SUBSYS_54108086&REV_59\185E0FFFFF353A5900
        MediaSubType        = 2

Interface {113B3CD4-0AAB-4EF6-8C18-2BC34E5BAC82}
LastWrite time Mon Apr 18 15:28:57 2016 (UTC)
        Name                = Local Area Connection* 9
        PnpInstanceID       =
        MediaSubType        =

Interface {157A11A7-FDC5-4AA5-A6DD-D614DC7EB54E}
LastWrite time Mon Apr 18 15:57:01 2016 (UTC)
        Name                = Local Area Connection* 13
        PnpInstanceID       =
        MediaSubType        =

Interface {18A41EC0-40B4-43EE-A035-2FF69FE3875E}
LastWrite time Mon Apr 18 15:57:01 2016 (UTC)
        Name                = Local Area Connection* 12
        PnpInstanceID       =
        MediaSubType        =

Interface {29898C9D-B0A4-4FEF-BDB6-57A562022CEE}
LastWrite time Sun Nov 21 03:39:55 2010 (UTC)
        Name                = Local Area Connection* 2
        PnpInstanceID       =
        MediaSubType        =

Interface {2A088A0C-A99B-4B11-81C8-178260EEB892}
LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
        Name                = Local Area Connection 3
        PnpInstanceID       = ROOT\NET\0001
        MediaSubType        =

Interface {2C5A5D75-A8A3-4ECF-ABCE-BB192A7E3A64}
LastWrite time Mon Apr 18 15:57:01 2016 (UTC)
        Name                = Local Area Connection* 14
        PnpInstanceID       =
        MediaSubType        =

Interface {2CAA64ED-BAA3-4473-B637-DEC65A14C8AA}
LastWrite time Tue Jul 14 04:53:20 2009 (UTC)
        Name                = Local Area Connection* 8
        PnpInstanceID       =
        MediaSubType        =

Interface {4525A64F-379A-4D68-8A81-DA5AA833E191}
LastWrite time Mon Apr 18 15:28:57 2016 (UTC)
        Name                = Bluetooth Network Connection
        PnpInstanceID       =
        MediaSubType        =

Interface {4A6E309E-FE5E-4D5C-9B3D-9E58803175CB}
LastWrite time Mon Apr 18 15:57:01 2016 (UTC)
Page 48

```
                              SYSTEM OUTPUT.txt
        Name                  = Local Area Connection* 15
        PnpInstanceID         =
        MediaSubType          =

Interface {4BA4B36E-29B2-45EB-8693-07A52C8F3CC5}
LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
        Name                  = Local Area Connection
        PnpInstanceID         =
PCI\VEN_8086&DEV_15A2&SUBSYS_062C1028&REV_03\3&11583659&0&C8
        MediaSubType          =

Interface {5BF54C7E-91DA-457D-80BF-333677D7E316}
LastWrite time Tue Jul 14 04:49:33 2009 (UTC)
        Name                  = Local Area Connection* 7
        PnpInstanceID         =
        MediaSubType          =

Interface {71F897D7-EB7C-4D8D-89DB-AC80D9DD2270}
LastWrite time Tue Jul 14 04:49:27 2009 (UTC)
        Name                  = Local Area Connection*
        PnpInstanceID         =
        MediaSubType          =

Interface {78032B7E-4968-42D3-9F37-287EA86C0AAA}
LastWrite time Tue Jul 14 05:09:03 2009 (UTC)
        Name                  = Local Area Connection* 10
        PnpInstanceID         =
        MediaSubType          =

Interface {7A4A7BB6-A99C-4488-BC73-BFFFAB0B53CC}
LastWrite time Mon Apr 18 15:57:04 2016 (UTC)
        Name                  = Local Area Connection* 16
        PnpInstanceID         =
        MediaSubType          =

Interface {8E301A52-AFFA-4F49-B9CA-C79096A1A056}
LastWrite time Tue Jul 14 04:49:32 2009 (UTC)
        Name                  = Local Area Connection* 5
        PnpInstanceID         =
        MediaSubType          =

Interface {915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3}
LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
        Name                  = Local Area Connection 2
        PnpInstanceID         = ROOT\NET\0000
        MediaSubType          =

Interface {957BCF87-92DE-4D58-8EFC-42A6CA2DEA60}
LastWrite time Mon Apr 18 15:56:56 2016 (UTC)
        Name                  = Reusable ISATAP Interface
{957BCF87-92DE-4D58-8EFC-42A6CA2DEA60}
        PnpInstanceID         =
        MediaSubType          =

Interface {9A399D81-2EAD-4F23-BCDD-637FC13DCD51}
LastWrite time Tue Jul 14 04:49:32 2009 (UTC)
        Name                  = Local Area Connection* 6
        PnpInstanceID         =
        MediaSubType          =

Interface {DF02E7DE-1391-4C75-ACCE-5406352E17E1}
LastWrite time Mon Apr 18 15:57:00 2016 (UTC)
        Name                  = Local Area Connection* 11
                              Page 49
```

```
                          SYSTEM OUTPUT.txt
        PnpInstanceID      =
        MediaSubType       =

Interface {DF4A9D2C-8742-4EB1-8703-D395C4183F33}
LastWrite time Tue Jul 14 04:49:31 2009 (UTC)
        Name               = Local Area Connection* 4
        PnpInstanceID      =
        MediaSubType       =

Interface {E43D242B-9EAB-4626-A952-46649FBB939A}
LastWrite time Tue Jul 14 04:49:30 2009 (UTC)
        Name               = Local Area Connection* 3
        PnpInstanceID      =
        MediaSubType       =


-------------------------------------------
nic v.20100401
(System) Gets NIC info from System hive

Adapter: {033026B9-7329-415D-8068-DD988B393525}
LastWrite Time: Mon Apr 18 15:28:03 2016 Z
    EnableDHCP            1

Adapter: {2A088A0C-A99B-4B11-81C8-178260EEB892}
LastWrite Time: Mon Apr 18 15:57:04 2016 Z
    EnableDHCP            1

Adapter: {4525A64F-379A-4D68-8A81-DA5AA833E191}
LastWrite Time: Mon Apr 18 15:28:58 2016 Z
    EnableDHCP            1

Adapter: {4BA4B36E-29B2-45EB-8693-07A52C8F3CC5}
LastWrite Time: Mon Apr 18 15:27:40 2016 Z
    EnableDHCP            0
  DefaultGateway

Adapter: {915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3}
LastWrite Time: Mon Apr 18 15:56:53 2016 Z
    EnableDHCP            1


-------------------------------------------
nic_mst2 v.20080324
(System) Gets NICs from System hive; looks for MediaType = 2

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

ControlSet001\Services\Tcpip\Parameters\Interfaces
LastWrite time Wed Apr 20 12:56:30 2016 (UTC)

Interface {2A088A0C-A99B-4B11-81C8-178260EEB892}
Name: Local Area Connection 3
Control\Network key LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
Services\Tcpip key LastWrite time Mon Apr 18 15:57:14 2016 (UTC)
        DhcpDomain      =
        DhcpIPAddress   =
        DhcpSubnetMask  =
        DhcpNameServer  =
        DhcpServer      =

Interface {915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3}
Name: Local Area Connection 2
Control\Network key LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
                          Page 50
```

```
                                SYSTEM OUTPUT.txt
Services\Tcpip key LastWrite time Mon Apr 18 15:57:14 2016 (UTC)
        DhcpDomain      =
        DhcpIPAddress   = 0.0.0.0
        DhcpSubnetMask = 255.0.0.0
        DhcpNameServer =
        DhcpServer      = 255.255.255.255


Interface {4BA4B36E-29B2-45EB-8693-07A52C8F3CC5}
Name: Local Area Connection
Control\Network key LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
Services\Tcpip key LastWrite time Wed Apr 20 16:57:57 2016 (UTC)
        DhcpDomain      = fda.gov
        DhcpIPAddress   = 10.125.5.188
        DhcpSubnetMask = 255.255.254.0
        DhcpNameServer = 10.185.42.30 10.208.42.30 10.185.42.31 10.176.32.50
        DhcpServer      = 10.177.16.54


Interface {033026B9-7329-415D-8068-DD988B393525}
Name: Wireless Network Connection
Control\Network key LastWrite time Mon Apr 18 16:26:11 2016 (UTC)
Services\Tcpip key LastWrite time Thu Apr 28 15:00:34 2016 (UTC)
        DhcpDomain      =
        DhcpIPAddress   = 0.0.0.0
        DhcpSubnetMask = 255.0.0.0
        DhcpNameServer =
        DhcpServer      = 255.255.255.255


------------------------------------------
nic2 v.20100401
(System) Gets NIC info from System hive

Adapter: {033026B9-7329-415D-8068-DD988B393525}
LastWrite Time: Thu Apr 28 15:00:34 2016 Z
    UseZeroBroadcast            0
    EnableDeadGWDetect          1
    EnableDHCP                  1
    NameServer
    Domain
    RegistrationEnabled         1
    RegisterAdapterName         0
    DhcpIPAddress               0.0.0.0
    DhcpSubnetMask              255.0.0.0
    DhcpServer                  255.255.255.255
    Lease                       0
    LeaseObtainedTime           Thu Jan  1 00:00:00 1970 Z
    T1                          Thu Jan  1 00:00:00 1970 Z
    T2                          Thu Jan  1 00:00:00 1970 Z
    LeaseTerminatesTime         Thu Jan  1 00:00:00 1970 Z
    AddressType                 0
    IsServerNapAware            0
    DhcpConnForceBroadcastFlag  0
    MTU                         1300
    DhcpNetworkHint             644414D275946494
    DhcpGatewayHardware
d    -     ⊡āÿüT
    DhcpGatewayHardwareCount    1

Adapter: {2A088A0C-A99B-4B11-81C8-178260EEB892}
LastWrite Time: Mon Apr 18 15:57:14 2016 Z
    UseZeroBroadcast            0
    EnableDeadGWDetect          1
    EnableDHCP                  1
    NameServer
                                Page 51
```

\

```
                        SYSTEM OUTPUT.txt
Domain
RegistrationEnabled           1
RegisterAdapterName           0
MTU                           1300

Adapter: {4525A64F-379A-4D68-8A81-DA5AA833E191}
LastWrite Time: Mon Apr 18 15:57:14 2016 Z
UseZeroBroadcast              0
EnableDeadGWDetect            1
EnableDHCP                    1
NameServer
Domain
RegistrationEnabled           1
RegisterAdapterName           0
DhcpIPAddress                 0.0.0.0
DhcpSubnetMask                255.0.0.0
DhcpServer                    255.255.255.255
Lease                         0
LeaseObtainedTime             Thu Jan  1 00:00:00 1970 Z
T1                            Thu Jan  1 00:00:00 1970 Z
T2                            Thu Jan  1 00:00:00 1970 Z
LeaseTerminatesTime           Thu Jan  1 00:00:00 1970 Z
AddressType                   0
IsServerNapAware              0
DhcpConnForceBroadcastFlag    0
MTU                           1300

Adapter: {4BA4B36E-29B2-45EB-8693-07A52C8F3CC5}
LastWrite Time: Wed Apr 20 16:57:57 2016 Z
UseZeroBroadcast              0
EnableDeadGWDetect            1
EnableDHCP                    1
NameServer
Domain
RegistrationEnabled           1
RegisterAdapterName           0
DhcpServer                    10.177.16.54
Lease                         1814396
LeaseObtainedTime             Wed Apr 20 16:36:29 2016 Z
T1                            Sun May  1 04:36:27 2016 Z
T2                            Mon May  9 01:36:25 2016 Z
LeaseTerminatesTime           Wed May 11 16:36:25 2016 Z
AddressType                   0
IsServerNapAware              0
DhcpConnForceBroadcastFlag    1
MTU                           1300
IPAddress
SubnetMask
DefaultGateway
DhcpIPAddress                 10.125.5.188
DhcpSubnetMask                255.255.254.0
DhcpInterfaceOptions          ,        ▯       _3w
Đ*
¹ *_          +          _3w
¹ *
Đ*
¹ *
° 2ᴸ         ⌐          _3w
}⌐ ☼     •          _3wfda.gov          ⌐          _3wÿÿÿþ 6          ⌐          _3w
w|⌐5              _3w|    ü                ⌐|WQ          ⊥          _3w
ÿÿOCL0166192.fda.gov   3       ⌐       _3w ←⌐|
DhcpGatewayHardware
}⌐  –   ß☼.⊥
```

Page 52

```
                                 SYSTEM OUTPUT.txt
    DhcpGatewayHardwareCount     1
    DhcpNameServer               10.185.42.30 10.208.42.30 10.185.42.31 10.176.32.50
    DhcpDefaultGateway           10.125.4.1
    DhcpDomain                   fda.gov
    DhcpSubnetMaskOpt            255.255.254.0

Adapter: {846ee342-7039-11de-9d20-806e6f6e6963}
LastWrite Time: Wed Apr 20 12:56:30 2016 Z

Adapter: {915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3}
LastWrite Time: Mon Apr 18 15:57:14 2016 Z
    UseZeroBroadcast             0
    EnableDeadGWDetect           1
    EnableDHCP                   1
    NameServer
    Domain
    RegistrationEnabled          1
    RegisterAdapterName          0
    DhcpIPAddress                0.0.0.0
    DhcpSubnetMask               255.0.0.0
    DhcpServer                   255.255.255.255
    Lease                        0
    LeaseObtainedTime            Thu Jan  1 00:00:00 1970 Z
    T1                           Thu Jan  1 00:00:00 1970 Z
    T2                           Thu Jan  1 00:00:00 1970 Z
    LeaseTerminatesTime          Thu Jan  1 00:00:00 1970 Z
    AddressType                  0
    IsServerNapAware             0
    DhcpConnForceBroadcastFlag   0
    MTU                          1300

----------------------------------------
nolmhash v.20100712
(System) Gets NoLMHash value

nolmhash v.20100712
ControlSet001\Control\Lsa
LastWrite: Wed Apr 20 15:40:54 2016

NoLMHash value = 1

A value of 1 indicates that LMHashes are not stored in the SAM.
----------------------------------------
pagefile v.20140505
(System) Get info on pagefile(s)

PagingFiles = ?:\pagefile.sys
ClearPageFileAtShutdown = 0
PagingFiles = ?:\pagefile.sys
----------------------------------------
prefetch v.20120914
(SYSTEM) Gets the the Prefetch Parameters

EnablePrefetcher     = 3

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled
----------------------------------------
productpolicy v.20091116
(System) Parse ProductPolicy value (Vista & Win2008 ONLY)
```

Page 53

SYSTEM OUTPUT.txt

Note: This plugin applies to Vista and Windows 2008 ONLY.
For a listing of names and values, see:
http://www.geoffchappell.com/viewer.htm?doc=notes/windows/license/install.htm&tx=3,5
,6;4


ACLUIFileFolderTool-IsSecurityUIEnabled - 1
ChangeDesktopBackground-Enabled - 1
DNS-Client-license-DAPolicy - 1
GroupPolicy-License-DomainIncapableSystem - 0
GroupPolicy-License-NetworkWaitTimeoutInSeconds - 30
GroupPolicy-License-WaitForNetwork - 0
IASLicensing-allowSubnetSyntax - 0
IASLicensing-maxClient - 0
IASLicensing-maxServerGroups - 0
Kernel-DynamicPartitioningSupported - 0
Kernel-ExpirationDate - 00000000000000000000000000000000
Kernel-MUI-Language-Allowed - EMPTY
Kernel-MUI-Language-Disallowed - EMPTY
Kernel-MUI-Language-SKU -
en-US;ar-SA;pt-BR;zh-TW;zh-CN;zh-HK;cs-CZ;da-DK;el-GR;es-ES;fi-FI;fr-FR;de-DE;he-IL;
hu-HU;it-IT;ja-JP;ko-KR;nl-NL;nb-NO;pl-PL;pt-PT;ru-RU;sv-SE;tr-TR;bg-BG;hr-HR;et-EE;
lv-LV;lt-LT;ro-RO;sr-Latn-CS;sk-SK;sl-SI;th-TH;uk-UA;fy-NL;qps-ploc;qps-plocm
Kernel-MUI-Number-Allowed - 1000
Kernel-MaxPhysicalPage - 4096
Kernel-MemoryMirroringSupported - 0
Kernel-NativeVHDBoot - 1
Kernel-PersistDefectiveMemoryList - 0
Kernel-PhysicalMemoryAddAllowed - 0
Kernel-ProductInfo - 4
Kernel-RegisteredProcessors - 2
Kernel-VirtualDynamicPartitioningSupported - 0
Kernel-VmPhysicalMemoryAddAllowed - 1
Kernel-WindowsMaxMemAllowedia64 - 196608
Kernel-WindowsMaxMemAllowedx64 - 196608
Kernel-WindowsMaxMemAllowedx86 - 4096
LSA-Credman-DisableDomainCreds - 0
LSA-Policy-EnableTrustedDomains - 0
MathRecognizerEventsLicensing-EnableMathRecognizer - 1
Microsoft-Windows-AuxiliaryDisplay-EnableAPI - 1
Microsoft-Windows-AuxiliaryDisplay-EnableCPL - 1
Microsoft-Windows-AuxiliaryDisplay-EnableDriver - 1
Microsoft-Windows-AuxiliaryDisplay-EnableSDP - 1
Microsoft-Windows-Core-AllowMultiMon - 1
Microsoft-Windows-Core-AllowedControlledDevicesForBoot - 12
Microsoft-Windows-Core-InstanceLimitExemptedApps -
Microsoft-Windows-Core-MaxConcurrentIApp - 0
Microsoft-Windows-Core-MaxHRes - 4294967295
Microsoft-Windows-Core-MaxTopLevelWinPerApp - 0
Microsoft-Windows-Core-MaxVRes - 4294967295
Microsoft-Windows-Core-NeedsFullOEMVerification - 1
Microsoft-Windows-Core-ParentProcessDenyList -
Microsoft-Windows-DOT11PREF-AllowAdhoc - 1
Microsoft-Windows-DesktopWindowManager-Core-AnimatedTransitionsAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-CompositionAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-Flip3dAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-LivePreviewAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-ThumbnailsAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-TransparencyAllowed - 1
Microsoft-Windows-HotStart-EnableHotStart - 1
Microsoft-Windows-IE-InternetExplorer-SupportEnableAutoUpgrade - 1
Microsoft-Windows-InternetConnectionSharingConfig-HomeNetBeacon - 1
Microsoft-Windows-InternetConnectionSharingConfig-HomeNetICS - 1
Page 54

SYSTEM OUTPUT.txt
```
Microsoft-Windows-NetworkBridge-WindowsHomeNwkEnabled - 1
Microsoft-Windows-OfflineFiles-Core-BranchCachingEnabled - 1
Microsoft-Windows-OfflineFiles-Core-FeatureEnabled - 1
Microsoft-Windows-QWAVE-EnableAdaptiveFlow - 1
Microsoft-Windows-QWAVE-Layer3Probing - 1
Microsoft-Windows-SensorsLicense-EnableCPL - 1
MicrosoftWindowsSafeDocsMain-BackupToNetShare - 1
MicrosoftWindowsSafeDocsMain-GPSupport - 1
MicrosoftWindowsSafeDocsMain-PerUserBackup - 1
MobilePCMobilityCenter-EnableMobilityCenter - 1
MobilePCPresentationSettings-EnablePresentationSettings - 1
NetworkProjection-CanRunNetworkProjection - 1
NetworkProjection-CanStartPresenting - 1
NetworkSecurity-IPsecDoSProtection-EnabledPolicy - 0
OMD-API-Enabled - 1
PeerDist-Common-Client-Enabled - 1
PeerDist-Common-HostedCache-Enabled - 0
PeerDist-Common-KMDriver-Enabled - 0
PeerDist-Common-Server-Enabled - 0
PeerToPeerBase-Collaboration-EnabledPolicy - 1
PeerToPeerBase-Graphing-EnabledPolicy - 1
PeerToPeerBase-Grouping-EnabledPolicy - 1
PeerToPeerBase-IdManager-EnabledPolicy - 1
PeerToPeerBase-Pnrp-EnabledPolicy - 1
Personalization-Enabled - 1
PhotoMinFeature-AdvancedSlideshow - 0
PhotoMinFeature-MakeDVD - 0
Printing-Spooler-Core-Localspl-Licensing-Enabled - 1
Printing-Spooler-Core-Spoolss-Licensing-Enabled - 1
Printing-Spooler-Core-Spoolss-Licensing-Network-Default-Printer-Enabled - 1
Printing-Spooler-Pmc-Licensing-Enabled - 1
RasBase-DefaultConnections - 2
RasBase-MaxConnections - 3
SLC-Component-SKU-OCUR-OCURControlContentAllowed - 0
SMBServer-AllowHashPublication - 0
SMBServer-AllowRemoteLegacyShadowCopyAccess - 1
SMBServer-AllowRemoteShadowCopyAccess - 1
SMBServer-WindowsMaxInSMBConns - 20
SecureStartupFeature-Enabled - 1
SecureStartupFeature-Enabled-Driver - 1
SecureStartupFeature-Enabled-Premium - 1
SecureStartupFeature-PerfWarning - 0
Security-SPP-ActivationResetCount - 5
Security-SPP-ActivationResetCountMax - 2147483647
Security-SPP-ApplicationActivationResetCount - 5
Security-SPP-ApplicationActivationResetCountMax - 2147483647
Security-SPP-CMIDExpirationPeriod - 43200
Security-SPP-EvaluationModeEnabled - 0
Security-SPP-GenuineLocalStatus - 1
Security-SPP-KmsCountedIdList -
Security-SPP-Reserved-EnableNotificationMode - 1
Security-SPP-Reserved-SkuPpdConsumed - 1
Security-SPP-Reserved-TBLProductKeyType - 0
Security-SPP-Reserved-TBLRemainingTime - 0
Security-SPP-Reserved-TBLState - 0
Security-SPP-TokenActivation-AdditionalInfo -
Security-SPP-UX-Slui-SelectivelySetBlackBackground - 1
SnippingToolLicensing-Enabled - 1
StickyNotesLicensing-Enabled - 1
TabletPC-MathInputLicensing-EnableMathInput - 1
TabletPC-UIHub-EnableCursors - 1
TabletPC-UIHub-EnableFeedback - 1
TabletPC-UIHub-EnableFlicks - 1
```
Page 55

SYSTEM OUTPUT.txt

```
TabletPC-tabbtn-EnableButtons - 1
TabletPCAccessories-EnableJournal - 1
TabletPCAccessories-EnableStickyNotes - 1
TabletPCCoreInkRecognitionLicensing-EnableText - 1
TabletPCInputPanel-EnableTIP - 1
TabletPCInputPanel-EnableTIPSynced - 1
TabletPCInputPersonalization-EnablePersonalization - 1
TabletPCPlatformInput-core-EnableTouchUI - 1
TabletPCPlatformInput-core-MultiTouchGestures - 1
TabletPCPlatformInput-core-SFP - 1
TerminalServices-DeviceRedirection-Licenses-PnpRedirectionAllowed - 1
TerminalServices-DeviceRedirection-Licenses-TSAudioCaptureAllowed - 1
TerminalServices-DeviceRedirection-Licenses-TSEasyPrintAllowed - 1
TerminalServices-DeviceRedirection-Licenses-TSMFPluginAllowed - 1
TerminalServices-RDP-7-Advanced-Compression-Allowed - 1
TerminalServices-RemoteApplications-ClientSku-RAILAllowed - 1
TerminalServices-RemoteConnectionManager-0f0a4bf8-8362-435d-938c-222a518a8b78-Disabl
ed - 0
TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-Localo
nly - 0
TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSes
sions - 1
TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-Initia
lProgram - %SystemRoot%\ehome\mcrmgr.exe
TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSes
sions - 5
TerminalServices-RemoteConnectionManager-AllowAppServerMode - 0
TerminalServices-RemoteConnectionManager-AllowD3DRemoting - 1
TerminalServices-RemoteConnectionManager-AllowMultimon - 1
TerminalServices-RemoteConnectionManager-AllowMultipleSessions - 1
TerminalServices-RemoteConnectionManager-AllowRemoteConnections - 1
TerminalServices-RemoteConnectionManager-MaxUserSessions - 0
TerminalServices-RemoteConnectionManager-UiEffects-DWMRemotingAllowed - 1
TerminalServices-RemoteConnectionManager-b7857721-7a62-4a37-aff3-253fe2b8b0e8-MaxSes
sions - 0
VirtualPC-licensing-Enabled - 1
VirtualXP-licensing-Enabled - 1
WMPPlayer-HMEAllowed - 1
WMPPlayer-RMEAllowed - 1
WMPPlayer-RMESecurityGroupAllowed - 0
WindowsSearchComponent-ComponentInstalled - 1
WorkstationService-DomainJoinEnabled - 1
appid-EnableV2 - 1
explorer-AeroAnimationAllowed - 1
explorer-AeroShakeAllowed - 1
feclient-EfsEnabled - 1
feclient-EfsUserCacheLimit - 5
msac3enc-DolbyDigitalEncoderV2AddIn - 0
msac3enc-DolbyDigitalEncoderV2AddInEnable - 1
msac3enc-DolbyDigitalEncoderV2InSKU - 1
msmpeg2adec-AACDecoderV2AddIn - 0
msmpeg2adec-AACDecoderV2AddInEnable - 1
msmpeg2adec-AACDecoderV2InSKU - 1
msmpeg2adec-DolbyDigitalDecoderV2AddIn - 0
msmpeg2adec-DolbyDigitalDecoderV2AddInEnable - 1
msmpeg2adec-DolbyDigitalDecoderV2InSKU - 1
msmpeg2enc-MPEG2VideoEncoderV2AddIn - 0
msmpeg2enc-MPEG2VideoEncoderV2AddInEnable - 1
msmpeg2enc-MPEG2VideoEncoderV2InSKU - 1
msmpeg2vdec-H264VideoDecoderV2AddIn - 0
msmpeg2vdec-H264VideoDecoderV2AddInEnable - 1
msmpeg2vdec-H264VideoDecoderV2InSKU - 1
msmpeg2vdec-MPEG2VideoDecoderV2AddIn - 0
```

Page 56

SYSTEM OUTPUT.txt
msmpeg2vdec-MPEG2VideoDecoderV2AddInEnable - 1
msmpeg2vdec-MPEG2VideoDecoderV2InSKU - 1
parentalcontrols-EnableFeature - 1
provsvc-license-HomeGroupCreate - 1
shell-homegroup-Enabled - 1
shell32-license-GroupPolicy-TryHarderPinned - 1
volmgrx-SupportDynamic - 1
volmgrx-SupportMirror - 1
volmgrx-SupportRaid5 - 0
----------------------------------------
producttype v.20100325
(System) Queries System hive for Windows Product info

ControlSet001\Control\ProductOptions
LastWrite = Mon Apr 18 15:51:15 2016

Ref: http://support.microsoft.com/kb/152078
     http://support.microsoft.com/kb/181412

ProductType   = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

ProductSuite = Terminal Server
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx
----------------------------------------
rdpport v.20100713
(System) Queries System hive for RDP Port

rdpport v.20100713

Remote Desktop Listening Port Number = 3389
----------------------------------------
routes v.20100817
(System) Get persistent routes

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
LastWrite: Sun Nov 21 03:39:53 2010

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes has no values.
----------------------------------------
safeboot v.20081216
(System) Check SafeBoot entries

Minimal   [Mon Apr 18 15:25:09 2016 Z]
Tue Jul 14 04:49:01 2009 Z
  Power (Service)
  ProfSvc (Service)
  WinDefend (Service)
Tue Jul 14 04:53:35 2009 Z
  AppInfo (Service)
  AppMgmt (Service)
  Base (Driver Group)
  Boot Bus Extender (Driver Group)
  Boot file system (Driver Group)
  CryptSvc (Service)
  DcomLaunch (Service)
  EFS (Service)
  EventLog (Service)
  File system (Driver Group)
  Filter (Driver Group)

Page 57

SYSTEM OUTPUT.txt

        HelpSvc (Service)
        KeyIso (Service)
        Netlogon (Service)
        NTDS (Service)
        PCI Configuration (Driver Group)
        PlugPlay (Service)
        PNP Filter (Driver Group)
        Primary disk (Driver Group)
        RpcEptMapper (Service)
        RpcSs (Service)
        sacsvr (Service)
        SCSI Class (Driver Group)
        sermouse.sys (Driver)
        SWPRV (Service)
        System Bus Extender (Driver Group)
        TabletInputService (Service)
        TBS (Service)
        TrustedInstaller (Service)
        VDS (Service)
        vga.sys (Driver)
        vgasave.sys (Driver)
        vmms (Service)
        volmgr.sys (Driver)
        volmgrx.sys (Driver)
        WinMgmt (Service)
        {36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)
        {4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)
        {4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)
        {4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)
        {4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)
        {4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)
        {4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)
        {4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)
        {4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)
        {4D36E97D-E325-11CE-BFC1-08002BE10318} (System)
        {4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)
        {533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)
        {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)
        {71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)
        {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)
        {D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)
        {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)
Tue Jul 14 04:54:07 2009 Z
        WudfPf (Driver)
        WudfRd (Driver)
        WudfSvc (Service)
Mon Apr 18 15:25:09 2016 Z
        Wdf01000.sys (Driver)

Network   [Mon Apr 18 16:00:47 2016 Z]
Tue Jul 14 04:49:01 2009 Z
        MPSDrv (Driver)
        MPSSvc (Service)
        Power (Service)
        ProfSvc (Service)
        WinDefend (Service)
Tue Jul 14 04:49:20 2009 Z
        NlaSvc (Service)
Tue Jul 14 04:53:35 2009 Z
        AFD (Service)
        AppInfo (Service)
        AppMgmt (Service)
        Base (Driver Group)

Page 58

SYSTEM OUTPUT.txt

BFE (Service)
Boot Bus Extender (Driver Group)
Boot file system (Driver Group)
bowser (Driver)
Browser (Service)
CryptSvc (Service)
DcomLaunch (Service)
dfsc (Driver)
Dhcp (Service)
DnsCache (Service)
Dot3Svc (Service)
Eaphost (Service)
EFS (Service)
EventLog (Service)
File system (Driver Group)
Filter (Driver Group)
HelpSvc (Service)
IKEEXT (Service)
ipnat.sys (Driver)
KeyIso (Service)
LanmanServer (Service)
LanmanWorkstation (Service)
LmHosts (Service)
Messenger (Service)
mrxsmb (Driver)
mrxsmb10 (Driver)
mrxsmb20 (Driver)
NativeWifiP (Service)
NDIS (Driver Group)
NDIS Wrapper (Driver Group)
Ndisuio (Service)
NetBIOS (Service)
NetBIOSGroup (Driver Group)
NetBT (Service)
NetDDEGroup (Driver Group)
Netlogon (Service)
NetMan (Service)
netprofm (Service)
Network (Driver Group)
NetworkProvider (Driver Group)
Nsi (Service)
nsiproxy.sys (Driver)
NTDS (Service)
PCI Configuration (Driver Group)
PlugPlay (Service)
PNP Filter (Driver Group)
PNP_TDI (Driver Group)
PolicyAgent (Service)
Primary disk (Driver Group)
rdbss (Driver)
rdpencdd.sys (Driver)
rdsessmgr (Service)
RpcEptMapper (Service)
RpcSs (Service)
sacsvr (Service)
SCardSvr (Service)
SCSI Class (Driver Group)
sermouse.sys (Driver)
SharedAccess (Service)
Streams Drivers (Driver Group)
SWPRV (Service)
System Bus Extender (Driver Group)
TabletInputService (Service)

Page 59

SYSTEM OUTPUT.txt

```
TBS (Service)
Tcpip (Service)
TDI (Driver Group)
TrustedInstaller (Service)
VDS (Service)
vga.sys (Driver)
vgasave.sys (Driver)
vmms (Service)
volmgr.sys (Driver)
volmgrx.sys (Driver)
WinMgmt (Service)
Wlansvc (Service)
WudfUsbccidDriver (Driver)
{36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)
{4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)
{4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)
{4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)
{4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)
{4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)
{4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)
{4D36E972-E325-11CE-BFC1-08002BE10318} (Net)
{4D36E973-E325-11CE-BFC1-08002BE10318} (NetClient)
{4D36E974-E325-11CE-BFC1-08002BE10318} (NetService)
{4D36E975-E325-11CE-BFC1-08002BE10318} (NetTrans)
{4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)
{4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)
{4D36E97D-E325-11CE-BFC1-08002BE10318} (System)
{4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)
{50DD5230-BA8A-11D1-BF5D-0000F805F530} (Smart card readers)
{533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)
{6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)
{71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)
{745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)
{D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)
{D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)
Tue Jul 14 04:53:49 2009 Z
  VaultSvc (Service)
Tue Jul 14 04:54:07 2009 Z
  WudfPf (Driver)
  WudfRd (Driver)
  WudfSvc (Service)
Tue Jul 14 04:54:37 2009 Z
  ndiscap (Driver)
Mon Apr 18 15:25:09 2016 Z
  Wdf01000.sys (Driver)
Mon Apr 18 15:54:46 2016 Z
  atashost (Service)
Mon Apr 18 15:58:30 2016 Z
  mfehidk.sys (Driver)
Mon Apr 18 16:00:31 2016 Z
  mfemms (Service)
Mon Apr 18 16:00:36 2016 Z
  mfehidk (Service)
  mfetdi2k (Service)
  mfetdi2k.sys (Driver)
  mfevtp (Service)
Mon Apr 18 16:00:40 2016 Z
  mfeaack (Service)
  mfeaack.sys (Driver)
Mon Apr 18 16:00:41 2016 Z
  mfeavfk (Service)
  mfeavfk.sys (Driver)
Mon Apr 18 16:00:43 2016 Z
```

Page 60

SYSTEM OUTPUT.txt

```
  mfefirek (Service)
  mfefirek.sys (Driver)
Mon Apr 18 16:00:47 2016 Z
  mfefire (Service)

-------------------------------------
services v.20080507
(System) Lists services/drivers in Services key by LastWrite times

ControlSet001\Services
Lists services/drivers in Services key by LastWrite times

Thu Apr 28 15:00:49 2016Z
  Name       = mferkdet
  Display    = McAfee Inc. mferkdet
  ImagePath  = system32\drivers\mferkdet.sys
  Type       = Kernel driver
  Start      = Manual
  Group      =

Thu Apr 28 15:00:38 2016Z
  Name       = mfeaack
  Display    = McAfee Inc. mfeaack
  ImagePath  = system32\drivers\mfeaack.sys
  Type       = Kernel driver
  Start      = Manual
  Group      =

Thu Apr 28 15:00:36 2016Z
  Name       = mfeapfk
  Display    = McAfee Inc. mfeapfk
  ImagePath  = system32\drivers\mfeapfk.sys
  Type       = Kernel driver
  Start      = Manual
  Group      =

Wed Apr 20 15:58:48 2016Z
  Name       = TrustedInstaller
  Display    = @%SystemRoot%\servicing\TrustedInstaller.exe,-100
  ImagePath  = %SystemRoot%\servicing\TrustedInstaller.exe
  Type       = Own_Process
  Start      = Manual
  Group      = ProfSvc_Group

Wed Apr 20 15:42:05 2016Z
  Name       = mfehidk
  Display    = McAfee Inc. mfehidk
  ImagePath  = system32\drivers\mfehidk.sys
  Type       = Kernel driver
  Start      = Boot Start
  Group      = FSFilter Anti-Virus

Wed Apr 20 15:42:04 2016Z
  Name       = DisplayLinkService
  Display    = DisplayLinkManager
  ImagePath  = "C:\Program Files\DisplayLink Core Software\DisplayLinkManager.exe"
  Type       = 0x0
  Start      = Auto Start
  Group      = PlugPlay

Wed Apr 20 15:41:02 2016Z
  Name       = AsyncMac
  Display    = @%systemroot%\system32\rascfg.dll,-32000
```

Page 61

```
                              SYSTEM OUTPUT.txt
    ImagePath = system32\DRIVERS\asyncmac.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

Wed Apr 20 15:40:59 2016Z
    Name      = mfeavfk
    Display   = McAfee Inc. mfeavfk
    ImagePath = system32\drivers\mfeavfk.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = mfeavfk01
    Display   = McAfee Inc.
    ImagePath =
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = mfemms
    Display   = McAfee Service Controller
    ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\\mfemms.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Wed Apr 20 15:40:52 2016Z
    Name      = cvusbdrv
    Display   = Dell ControlVault
    ImagePath = System32\Drivers\cvusbdrv.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Base

    Name      = kbdhid
    Display   = Keyboard HID Driver
    ImagePath = system32\DRIVERS\kbdhid.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Keyboard Port

    Name      = mouhid
    Display   = Mouse HID Driver
    ImagePath = system32\DRIVERS\mouhid.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Pointer Port

    Name      = scfilter
    Display   = @%SystemRoot%\System32\drivers\scfilter.sys,-11
    ImagePath = System32\DRIVERS\scfilter.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = PnP Filter

    Name      = WinUsb
    Display   = WinUSB Driver
    ImagePath = system32\DRIVERS\WinUSB.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Base
```

Page 62

SYSTEM OUTPUT.txt

```
Wed Apr 20 15:40:51 2016Z
   Name       = HidUsb
   Display    = Microsoft HID Class Driver
   ImagePath  = system32\DRIVERS\hidusb.sys
   Type       = Kernel driver
   Start      = Manual
   Group      = extended base

   Name       = monitor
   Display    = Microsoft Monitor Class Function Driver Service
   ImagePath  = system32\DRIVERS\monitor.sys
   Type       = Kernel driver
   Start      = Manual
   Group      =

   Name       = usbccgp
   Display    = Microsoft USB Generic Parent Driver
   ImagePath  = system32\DRIVERS\usbccgp.sys
   Type       = Kernel driver
   Start      = Manual
   Group      = Base

   Name       = usbvideo
   Display    = USB Video Device (WDM)
   ImagePath  = System32\Drivers\usbvideo.sys
   Type       = Kernel driver
   Start      = Manual
   Group      =

Wed Apr 20 15:40:50 2016Z
   Name       = mfefirek
   Display    = McAfee Inc. mfefirek
   ImagePath  = system32\drivers\mfefirek.sys
   Type       = Kernel driver
   Start      = Manual
   Group      =

Wed Apr 20 15:40:49 2016Z
   Name       = IntcAzAudAddService
   Display    = Service for Realtek HD Audio (WDM)
   ImagePath  = system32\drivers\RTDVHD64.sys
   Type       = Kernel driver
   Start      = Manual
   Group      =

   Name       = iusb3hub
   Display    = Intel(R) USB 3.0 Hub Driver
   ImagePath  = system32\DRIVERS\iusb3hub.sys
   Type       = Kernel driver
   Start      = Manual
   Group      = Base

   Name       = ST_Accel
   Display    = STMicroelectronics Accelerometer Service
   ImagePath  = system32\DRIVERS\ST_Accel.sys
   Type       = Kernel driver
   Start      = Manual
   Group      =

Wed Apr 20 15:40:48 2016Z
   Name       = IntcDAud
   Display    = Intel(R) Display Audio
   ImagePath  = system32\DRIVERS\IntcDAud.sys
```

Page 63

SYSTEM OUTPUT.txt

```
Type       = Kernel driver
Start      = Manual
Group      =

Name       = ksthunk
Display    = Kernel Streaming Thunks
ImagePath  = \SystemRoot\system32\drivers\ksthunk.sys
Type       = Kernel driver
Start      = Manual
Group      = PNP Filter

Name       = Parport
Display    = Parallel port driver
ImagePath  = system32\DRIVERS\parport.sys
Type       = Kernel driver
Start      = Manual
Group      = Parallel arbitrator

Name       = usbhub
Display    = Microsoft USB Standard Hub Driver
ImagePath  = system32\DRIVERS\usbhub.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Wed Apr 20 15:40:47 2016Z
Name       = mssmbios
Display    = Microsoft System Management BIOS Driver
ImagePath  = system32\DRIVERS\mssmbios.sys
Type       = Kernel driver
Start      = System Start
Group      =

Wed Apr 20 15:40:46 2016Z
Name       = nvlddmkm
Display    =
ImagePath  = system32\DRIVERS\nvlddmkm.sys
Type       = Kernel driver
Start      = Manual
Group      = Video

Name       = rdyboost
Display    = ReadyBoost
ImagePath  = System32\drivers\rdyboost.sys
Type       = Kernel driver
Start      = Boot Start
Group      = PnP Filter

Wed Apr 20 15:40:45 2016Z
Name       = ACPI
Display    = Microsoft ACPI Driver
ImagePath  = system32\drivers\ACPI.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Boot Bus Extender

Name       = acsock
Display    = acsock
ImagePath  = system32\DRIVERS\acsock64.sys
Type       = Kernel driver
Start      = Manual
Group      =
```

Page 64

```
                          SYSTEM OUTPUT.txt
Name       = AFD
Display    = @%systemroot%\system32\drivers\afd.sys,-1000
ImagePath  = \SystemRoot\system32\drivers\afd.sys
Type       = Kernel driver
Start      = System Start
Group      = PNP_TDI

Name       = ApfiltrService
Display    = Alps Touch Pad Filter Driver for Windows x64
ImagePath  = system32\DRIVERS\Apfiltr.sys
Type       = Kernel driver
Start      = Manual
Group      = Pointer Port

Name       = Beep
Display    = Beep
ImagePath  =
Type       = Kernel driver
Start      = System Start
Group      = Base

Name       = blbdrive
Display    =
ImagePath  = system32\DRIVERS\blbdrive.sys
Type       = Kernel driver
Start      = System Start
Group      =

Name       = bowser
Display    = @%systemroot%\system32\browser.dll,-102
ImagePath  = system32\DRIVERS\bowser.sys
Type       = File system driver
Start      = Manual
Group      = Network

Name       = CipcCdp
Display    = Cisco IP Communicator driver for CDP
ImagePath  = system32\DRIVERS\CipcCdp.sys
Type       = Kernel driver
Start      = Auto Start
Group      = NDIS

Name       = CLFS
Display    = @%SystemRoot%\system32\clfs.sys,-100
ImagePath  = System32\CLFS.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Filter

Name       = CmBatt
Display    = Microsoft ACPI Control Method Battery Driver
ImagePath  = system32\DRIVERS\CmBatt.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = CNG
Display    =
ImagePath  = System32\Drivers\cng.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Base
```

Page 65

SYSTEM OUTPUT.txt

```
Name        = Compbatt
Display     = Microsoft Composite Battery Driver
ImagePath   = system32\DRIVERS\compbatt.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Bus Extender

Name        = CompositeBus
Display     = Composite Bus Enumerator Driver
ImagePath   = system32\DRIVERS\CompositeBus.sys
Type        = Kernel driver
Start       = Manual
Group       = Extended Base

Name        = CSC
Display     = @%systemroot%\system32\cscsvc.dll,-202
ImagePath   = system32\drivers\csc.sys
Type        = Kernel driver
Start       = System Start
Group       = network

Name        = ctxusbm
Display     = Citrix USB Monitor Driver
ImagePath   = system32\DRIVERS\ctxusbm.sys
Type        = Kernel driver
Start       = System Start
Group       =

Name        = CVirtA
Display     = Cisco Systems VPN Adapter for 64-bit Windows
ImagePath   = system32\DRIVERS\CVirtA64.sys
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Name        = CVPNDRVA
Display     = Cisco Systems Inc. IPSec Driver
ImagePath   = \??\C:\WINDOWS\system32\Drivers\CVPNDRVA.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = DfsC
Display     = @%systemroot%\system32\drivers\dfsc.sys,-101
ImagePath   = System32\Drivers\dfsc.sys
Type        = File system driver
Start       = System Start
Group       = Network

Name        = discache
Display     = @%systemroot%\system32\drivers\discache.sys,-102
ImagePath   = System32\drivers\discache.sys
Type        = Kernel driver
Start       = System Start
Group       =

Name        = Disk
Display     = Disk Driver
ImagePath   = system32\drivers\disk.sys
Type        = Kernel driver
Start       = Boot Start
Group       =
```

Page 66

SYSTEM OUTPUT.txt

```
Name        = DNE
Display     = Deterministic Network Enhancer Miniport
ImagePath   = system32\DRIVERS\dne64x.sys
Type        = Kernel driver
Start       = Manual
Group       = PNP_TDI

Name        = dptf_acpi
Display     =
ImagePath   = system32\DRIVERS\dptf_acpi.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Name        = dptf_cpu
Display     =
ImagePath   = system32\DRIVERS\dptf_cpu.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Name        = DXGKrnl
Display     = LDDM Graphics Subsystem
ImagePath   = \SystemRoot\System32\drivers\dxgkrnl.sys
Type        = Kernel driver
Start       = Manual
Group       = Video Init

Name        = e1dexpress
Display     = Intel(R) PRO/1000 PCI Express Network Connection Driver D
ImagePath   = system32\DRIVERS\e1d62x64.sys
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Name        = enstart64_
Display     = enstart64_
ImagePath   = \??\C:\WINDOWS\system32\enstart64_.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = esif_lf
Display     =
ImagePath   = system32\DRIVERS\esif_lf.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Name        = FileInfo
Display     = @%SystemRoot%\system32\drivers\fileinfo.sys,-100
ImagePath   = system32\drivers\fileinfo.sys
Type        = File system driver
Start       = Boot Start
Group       = FSFilter Bottom

Name        = FltMgr
Display     = @%SystemRoot%\system32\drivers\fltmgr.sys,-10001
ImagePath   = system32\drivers\fltmgr.sys
Type        = File system driver
Start       = Boot Start
Group       = FSFilter Infrastructure
```

Page 67

SYSTEM OUTPUT.txt
```
Name        = Fs_Rec
Display     =
ImagePath   =
Type        = 0x0
Start       = Boot Start
Group       = File System

Name        = fvevol
Display     = @%SystemRoot%\system32\drivers\fvevol.sys,-100
ImagePath   = System32\DRIVERS\fvevol.sys
Type        = Kernel driver
Start       = Boot Start
Group       = PnP Filter

Name        = HDAudBus
Display     = Microsoft UAA Bus Driver for High Definition Audio
ImagePath   = system32\DRIVERS\HDAudBus.sys
Type        = Kernel driver
Start       = Manual
Group       = Extended Base

Name        = HTTP
Display     = @%SystemRoot%\system32\drivers\http.sys,-1
ImagePath   = system32\drivers\HTTP.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = hwpolicy
Display     = @%systemroot%\system32\drivers\hwpolicy.sys,-101
ImagePath   = System32\drivers\hwpolicy.sys
Type        = Kernel driver
Start       = Boot Start
Group       =

Name        = i8042prt
Display     = i8042 Keyboard and PS/2 Mouse Port Driver
ImagePath   = system32\DRIVERS\i8042prt.sys
Type        = Kernel driver
Start       = Manual
Group       = Keyboard Port

Name        = iaStorA
Display     =
ImagePath   = system32\drivers\iaStorA.sys
Type        = Kernel driver
Start       = Boot Start
Group       = SCSI miniport

Name        = iaStorF
Display     =
ImagePath   = system32\drivers\iaStorF.sys
Type        = Kernel driver
Start       = Boot Start
Group       =

Name        = igfx
Display     =
ImagePath   = system32\DRIVERS\igdkmd64.sys
Type        = Kernel driver
Start       = Manual
Group       = Video
```

Page 68

SYSTEM OUTPUT.txt

```
Name       = intelppm
Display    = Intel Processor Driver
ImagePath  = system32\DRIVERS\intelppm.sys
Type       = Kernel driver
Start      = Manual
Group      = Extended Base

Name       = iusb3xhc
Display    = Intel(R) USB 3.0 eXtensible Host Controller Driver
ImagePath  = system32\DRIVERS\iusb3xhc.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Name       = kbdclass
Display    = Keyboard Class Driver
ImagePath  = system32\DRIVERS\kbdclass.sys
Type       = Kernel driver
Start      = Manual
Group      = Keyboard Class

Name       = KSecDD
Display    =
ImagePath  = System32\Drivers\ksecdd.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Base

Name       = KSecPkg
Display    =
ImagePath  = System32\Drivers\ksecpkg.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Cryptography

Name       = lltdio
Display    = Link-Layer Topology Discovery Mapper I/O Driver
ImagePath  = system32\DRIVERS\lltdio.sys
Type       = Kernel driver
Start      = Auto Start
Group      = NDIS

Name       = luafv
Display    = @%systemroot%\system32\drivers\luafv.sys,-100
ImagePath  = \SystemRoot\system32\drivers\luafv.sys
Type       = File system driver
Start      = Auto Start
Group      = FSFilter Virtualization

Name       = MEIx64
Display    = Intel(R) Management Engine Interface
ImagePath  = system32\DRIVERS\TeeDriverx64.sys
Type       = Kernel driver
Start      = Manual
Group      = Extended Base

Name       = mfenlfk
Display    = McAfee NDIS Light Filter
ImagePath  = system32\DRIVERS\mfenlfk.sys
Type       = Kernel driver
Start      = System Start
Group      = NDIS
```

Page 69

SYSTEM OUTPUT.txt

```
Name      = mfewfpk
Display   = McAfee Inc. mfewfpk
ImagePath = system32\drivers\mfewfpk.sys
Type      = Kernel driver
Start     = Boot Start
Group     = PNP_TDI

Name      = mouclass
Display   = Mouse Class Driver
ImagePath = system32\DRIVERS\mouclass.sys
Type      = Kernel driver
Start     = Manual
Group     = Pointer Class

Name      = mountmgr
Display   = @%SystemRoot%\system32\drivers\mountmgr.sys,-100
ImagePath = System32\drivers\mountmgr.sys
Type      = Kernel driver
Start     = Boot Start
Group     = System Bus Extender

Name      = mpsdrv
Display   = @%SystemRoot%\system32\FirewallAPI.dll,-23092
ImagePath = System32\drivers\mpsdrv.sys
Type      = Kernel driver
Start     = Manual
Group     = network

Name      = MRxDAV
Display   = @%systemroot%\system32\webclnt.dll,-104
ImagePath = \SystemRoot\system32\drivers\mrxdav.sys
Type      = File system driver
Start     = Manual
Group     =

Name      = mrxsmb
Display   = @%systemroot%\system32\wkssvc.dll,-1002
ImagePath = system32\DRIVERS\mrxsmb.sys
Type      = File system driver
Start     = Manual
Group     = Network

Name      = mrxsmb10
Display   = @%systemroot%\system32\wkssvc.dll,-1004
ImagePath = system32\DRIVERS\mrxsmb10.sys
Type      = File system driver
Start     = Manual
Group     = Network

Name      = mrxsmb20
Display   = @%systemroot%\system32\wkssvc.dll,-1006
ImagePath = system32\DRIVERS\mrxsmb20.sys
Type      = File system driver
Start     = Manual
Group     = Network

Name      = Msfs
Display   =
ImagePath =
Type      = File system driver
Start     = System Start
Group     = File system
```

Page 70

SYSTEM OUTPUT.txt

```
Name       = msisadrv
Display    =
ImagePath  = system32\drivers\msisadrv.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Boot Bus Extender

Name       = Mup
Display    = @%systemroot%\system32\drivers\mup.sys,-101
ImagePath  = System32\Drivers\mup.sys
Type       = File system driver
Start      = Boot Start
Group      = Network

Name       = NativeWifiP
Display    = NativeWiFi Filter
ImagePath  = system32\DRIVERS\nwifi.sys
Type       = Kernel driver
Start      = Manual
Group      = NDIS

Name       = NDIS
Display    = @%SystemRoot%\system32\drivers\ndis.sys,-200
ImagePath  = system32\drivers\ndis.sys
Type       = Kernel driver
Start      = Boot Start
Group      = NDIS Wrapper

Name       = NdisTapi
Display    = @%systemroot%\system32\rascfg.dll,-32001
ImagePath  = system32\DRIVERS\ndistapi.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = Ndisuio
Display    = NDIS Usermode I/O Protocol
ImagePath  = system32\DRIVERS\ndisuio.sys
Type       = Kernel driver
Start      = Manual
Group      = NDIS

Name       = NdisWan
Display    = @%systemroot%\system32\rascfg.dll,-32002
ImagePath  = system32\DRIVERS\ndiswan.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = NDProxy
Display    = NDIS Proxy
ImagePath  =
Type       = Kernel driver
Start      = Manual
Group      = PNP_TDI

Name       = NetBIOS
Display    = NetBIOS Interface
ImagePath  = system32\DRIVERS\netbios.sys
Type       = File system driver
Start      = System Start
Group      = NetBIOSGroup
```

Page 71

SYSTEM OUTPUT.txt

```
Name      = NetBT
Display   = @%SystemRoot%\system32\drivers\netbt.sys,-2
ImagePath = System32\DRIVERS\netbt.sys
Type      = Kernel driver
Start     = System Start
Group     = PNP_TDI

Name      = NETwNs64
Display   = ___ Intel(R) Wireless Adapter Driver for Windows 7 - 64 Bit
ImagePath = system32\DRIVERS\Netwsw02.sys
Type      = Kernel driver
Start     = Manual
Group     = NDIS

Name      = Npfs
Display   =
ImagePath =
Type      = File system driver
Start     = System Start
Group     = File system

Name      = nsiproxy
Display   = @%SystemRoot%\system32\drivers\nsiproxy.sys,-2
ImagePath = system32\drivers\nsiproxy.sys
Type      = Kernel driver
Start     = System Start
Group     =

Name      = Ntfs
Display   =
ImagePath =
Type      = File system driver
Start     = Manual
Group     = Boot File System

Name      = Null
Display   =
ImagePath =
Type      = Kernel driver
Start     = System Start
Group     = Base

Name      = nvpciflt
Display   =
ImagePath = system32\DRIVERS\nvpciflt.sys
Type      = Kernel driver
Start     = Boot Start
Group     =

Name      = O2FJ2RDR
Display   =
ImagePath = system32\DRIVERS\O2FJ2w7x64.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = partmgr
Display   = @%SystemRoot%\system32\drivers\partmgr.sys,-100
ImagePath = System32\drivers\partmgr.sys
Type      = Kernel driver
Start     = Boot Start
Group     = Boot Bus Extender
```

Page 72

```
                            SYSTEM OUTPUT.txt
Name      = pci
Display   = PCI Bus Driver
ImagePath = system32\drivers\pci.sys
Type      = Kernel driver
Start     = Boot Start
Group     = Boot Bus Extender

Name      = pcw
Display   = Performance Counters for Windows Driver
ImagePath = System32\drivers\pcw.sys
Type      = Kernel driver
Start     = Boot Start
Group     = Base

Name      = PEAUTH
Display   = PEAUTH
ImagePath = system32\drivers\peauth.sys
Type      = Kernel driver
Start     = Auto Start
Group     =

Name      = PptpMiniport
Display   = @%systemroot%\system32\rascfg.dll,-32006
ImagePath = system32\DRIVERS\raspptp.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = prepdrvr
Display   = SMS Process Event Driver
ImagePath = system32\DRIVERS\prepdrv.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = prot_2k
Display   =
ImagePath =
Type      = Kernel driver
Start     = Boot Start
Group     =

Name      = Psched
Display   = @%SystemRoot%\System32\drivers\pacer.sys,-101
ImagePath = system32\DRIVERS\pacer.sys
Type      = Kernel driver
Start     = System Start
Group     = NDIS

Name      = RasAgileVpn
Display   = WAN Miniport (IKEv2)
ImagePath = system32\DRIVERS\AgileVpn.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = Rasl2tp
Display   = @%systemroot%\system32\rascfg.dll,-32005
ImagePath = system32\DRIVERS\rasl2tp.sys
Type      = Kernel driver
Start     = Manual
Group     =
```

Page 73

```
                        SYSTEM OUTPUT.txt
Name       = RasPppoe
Display    = @%systemroot%\system32\rascfg.dll,-32007
ImagePath  = system32\DRIVERS\raspppoe.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = RasSstp
Display    = @%systemroot%\system32\sstpsvc.dll,-202
ImagePath  = system32\DRIVERS\rassstp.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = rdbss
Display    = @%systemroot%\system32\wkssvc.dll,-1000
ImagePath  = system32\DRIVERS\rdbss.sys
Type       = File system driver
Start      = System Start
Group      = Network

Name       = rdpbus
Display    = Remote Desktop Device Redirector Bus Driver
ImagePath  = system32\DRIVERS\rdpbus.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = RDPCDD
Display    = @%systemroot%\system32\DRIVERS\RDPCDD.sys,-100
ImagePath  = System32\DRIVERS\RDPCDD.sys
Type       = Kernel driver
Start      = System Start
Group      = Video Save

Name       = RDPDR
Display    = Terminal Server Device Redirector Driver
ImagePath  = System32\drivers\rdpdr.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = RDPENCDD
Display    = @%systemroot%\system32\drivers\RDPENCDD.sys,-101
ImagePath  = system32\drivers\rdpencdd.sys
Type       = Kernel driver
Start      = System Start
Group      = Video Save

Name       = RDPREFMP
Display    = @%systemroot%\system32\drivers\RdpRefMp.sys,-101
ImagePath  = system32\drivers\rdprefmp.sys
Type       = Kernel driver
Start      = System Start
Group      = Video Save

Name       = RDPWD
Display    = RDP Winstation Driver
ImagePath  =
Type       = Kernel driver
Start      = Manual
Group      =
```

Page 74

SYSTEM OUTPUT.txt

```
Name       = rspndr
Display    = Link-Layer Topology Discovery Responder
ImagePath  = system32\DRIVERS\rspndr.sys
Type       = Kernel driver
Start      = Auto Start
Group      = NDIS

Name       = Serenum
Display    = Serenum Filter Driver
ImagePath  = system32\DRIVERS\serenum.sys
Type       = Kernel driver
Start      = Manual
Group      = PNP Filter

Name       = Serial
Display    = Serial port driver
ImagePath  = system32\DRIVERS\serial.sys
Type       = Kernel driver
Start      = System Start
Group      = Extended base

Name       = spldr
Display    = Security Processor Loader Driver
ImagePath  =
Type       = Kernel driver
Start      = Boot Start
Group      =

Name       = srv
Display    = @%systemroot%\system32\srvsvc.dll,-102
ImagePath  = System32\DRIVERS\srv.sys
Type       = File system driver
Start      = Manual
Group      = Network

Name       = srv2
Display    = @%systemroot%\system32\srvsvc.dll,-104
ImagePath  = System32\DRIVERS\srv2.sys
Type       = File system driver
Start      = Manual
Group      = Network

Name       = srvnet
Display    =
ImagePath  = System32\DRIVERS\srvnet.sys
Type       = File system driver
Start      = Manual
Group      = Network

Name       = stdcfltn
Display    = Disk Class Filter Driver for Accelerometer
ImagePath  = system32\DRIVERS\stdcfltn.sys
Type       = Kernel driver
Start      = Boot Start
Group      = PnP Filter

Name       = swenum
Display    = Software Bus Driver
ImagePath  = system32\DRIVERS\swenum.sys
Type       = Kernel driver
Start      = Manual
Group      =
```

Page 75

SYSTEM OUTPUT.txt

```
Name        = Tcpip
Display     = @%SystemRoot%\system32\tcpipcfg.dll,-50003
ImagePath   = System32\drivers\tcpip.sys
Type        = Kernel driver
Start       = Boot Start
Group       = PNP_TDI

Name        = tcpipreg
Display     = TCP/IP Registry Compatibility
ImagePath   = System32\drivers\tcpipreg.sys
Type        = Kernel driver
Start       = Auto Start
Group       =

Name        = TDTCP
Display     = TDTCP
ImagePath   = system32\drivers\tdtcp.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = tdx
Display     = @%SystemRoot%\system32\tcpipcfg.dll,-50004
ImagePath   = system32\DRIVERS\tdx.sys
Type        = Kernel driver
Start       = System Start
Group       = PNP_TDI

Name        = TermDD
Display     = Terminal Device Driver
ImagePath   = system32\DRIVERS\termdd.sys
Type        = Kernel driver
Start       = System Start
Group       =

Name        = tssecsrv
Display     = @%SystemRoot%\System32\DRIVERS\tssecsrv.sys,-101
ImagePath   = System32\DRIVERS\tssecsrv.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = tunnel
Display     = Microsoft Tunnel Miniport Adapter Driver
ImagePath   = system32\DRIVERS\tunnel.sys
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Name        = umbus
Display     = UMBus Enumerator Driver
ImagePath   = system32\DRIVERS\umbus.sys
Type        = Kernel driver
Start       = Manual
Group       = Extended Base

Name        = usbehci
Display     = Microsoft USB 2.0 Enhanced Host Controller Miniport Driver
ImagePath   = system32\DRIVERS\usbehci.sys
Type        = Kernel driver
Start       = Manual
Group       = Base
```

Page 76

```
                                     SYSTEM OUTPUT.txt
Name       = vdrvroot
Display    = Microsoft Virtual Drive Enumerator Driver
ImagePath  = system32\drivers\vdrvroot.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Boot Bus Extender

Name       = VgaSave
Display    =
ImagePath  = \SystemRoot\System32\drivers\vga.sys
Type       = Kernel driver
Start      = System Start
Group      = Video Save

Name       = volmgr
Display    = Volume Manager Driver
ImagePath  = system32\drivers\volmgr.sys
Type       = Kernel driver
Start      = Boot Start
Group      = System Bus Extender

Name       = volmgrx
Display    = @%SystemRoot%\system32\drivers\volmgrx.sys,-100
ImagePath  = System32\drivers\volmgrx.sys
Type       = Kernel driver
Start      = Boot Start
Group      = System Bus Extender

Name       = volsnap
Display    = Storage volumes
ImagePath  = system32\drivers\volsnap.sys
Type       = Kernel driver
Start      = Boot Start
Group      =

Name       = vpnva
Display    = Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for
Windows x64
ImagePath  = system32\DRIVERS\vpnva64-6.sys
Type       = Kernel driver
Start      = Manual
Group      = NDIS

Name       = vwifibus
Display    = Virtual WiFi Bus Driver
ImagePath  = system32\DRIVERS\vwifibus.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = vwififlt
Display    = Virtual WiFi Filter Driver
ImagePath  = system32\DRIVERS\vwififlt.sys
Type       = Kernel driver
Start      = System Start
Group      = NDIS

Name       = Wanarpv6
Display    = @%systemroot%\system32\rascfg.dll,-32012
ImagePath  = system32\DRIVERS\wanarp.sys
Type       = Kernel driver
Start      = System Start
Group      =
                                     Page 77
```

SYSTEM OUTPUT.txt

```
Name        = Wdf01000
Display     = @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000
ImagePath   = system32\drivers\Wdf01000.sys
Type        = Kernel driver
Start       = Boot Start
Group       = WdfLoadGroup

Name        = WfpLwf
Display     = WFP Lightweight Filter
ImagePath   = system32\DRIVERS\wfplwf.sys
Type        = Kernel driver
Start       = System Start
Group       = NDIS

Name        = WmiAcpi
Display     = Microsoft Windows Management Interface for ACPI
ImagePath   = system32\DRIVERS\wmiacpi.sys
Type        = Kernel driver
Start       = Manual
Group       = Extended Base

Name        = WudfPf
Display     = @%SystemRoot%\system32\drivers\Wudfpf.sys,-1000
ImagePath   = system32\drivers\WudfPf.sys
Type        = Kernel driver
Start       = Manual
Group       = base

Name        = WUDFRd
Display     = Windows Driver Foundation - User-mode Driver Framework Reflector
ImagePath   = system32\DRIVERS\WUDFRd.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Wed Apr 20 15:39:52 2016Z
Name        = drmkaud
Display     = Microsoft Trusted Audio Drivers
ImagePath   = \SystemRoot\system32\drivers\drmkaud.sys
Type        = Kernel driver
Start       = Manual
Group       =

Wed Apr 20 13:19:57 2016Z
Name        = macmnsvc
Display     = McAfee Agent Common Services
ImagePath   = "C:\Program Files (x86)\McAfee\Common Framework\macmnsvc.exe"
/ServiceStart
Type        = Own_Process
Start       = Auto Start
Group       =

Name        = masvc
Display     = McAfee Agent Service
ImagePath   = "C:\Program Files (x86)\McAfee\Common Framework\masvc.exe"
/ServiceStart
Type        = Own_Process
Start       = Auto Start
Group       =

Name        = McAfeeFramework
Display     = McAfee Agent Backwards Compatibility Service
```

Page 78

```
                           SYSTEM OUTPUT.txt
    ImagePath = "C:\Program Files (x86)\McAfee\Common Framework\x86\macompatsvc.exe"
    Type      = Own_Process
    Start     = Manual
    Group     =

Wed Apr 20 13:19:43 2016Z
    Name      = mfefire
    Display   = McAfee Firewall Core Service
    ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\\mfefire.exe"
    Type      = Own_Process
    Start     = Manual
    Group     =

Wed Apr 20 13:19:40 2016Z
    Name      = McShield
    Display   = McAfee McShield
    ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\\mcshield.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Wed Apr 20 13:19:38 2016Z
    Name      = mfevtp
    Display   = McAfee Validation Trust Protection Service
    ImagePath = "C:\WINDOWS\system32\mfevtps.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Wed Apr 20 13:19:10 2016Z
    Name      = enterceptAgent
    Display   = McAfee Host Intrusion Prevention Service
    ImagePath = "C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Tue Apr 19 20:40:52 2016Z
    Name      = MozillaMaintenance
    Display   = Mozilla Maintenance Service
    ImagePath = "C:\Program Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe"
    Type      = Own_Process
    Start     = Manual
    Group     =

Tue Apr 19 20:40:07 2016Z
    Name      = gupdate
    Display   = Google Update Service (gupdate)
    ImagePath = "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
    Type      = Own_Process
    Start     = Auto Start
    Group     =

    Name      = gupdatem
    Display   = Google Update Service (gupdatem)
    ImagePath = "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc
    Type      = Own_Process
    Start     = Manual
    Group     =

Tue Apr 19 20:03:56 2016Z
    Name      = MSDTC
```

Page 79

```
                               SYSTEM OUTPUT.txt
    Display    = @comres.dll,-2797
    ImagePath = %SystemRoot%\System32\msdtc.exe
    Type       = Own_Process
    Start      = Manual
    Group      =

Tue Apr 19 20:00:35 2016Z
    Name       = CmRcService
    Display    = Configuration Manager Remote Control
    ImagePath = C:\WINDOWS\CCM\RemCtrl\CmRcService.exe
    Type       = Own_Process
    Start      = Auto Start
    Group      =

Tue Apr 19 20:00:19 2016Z
    Name       = CcmFramework
    Display    =
    ImagePath =
    Type       =
    Start      =
    Group      =

Tue Apr 19 19:48:22 2016Z
    Name       = USBSTOR
    Display    = USB Mass Storage Driver
    ImagePath = system32\DRIVERS\USBSTOR.SYS
    Type       = Kernel driver
    Start      = Manual
    Group      =

Tue Apr 19 19:47:44 2016Z
    Name       = EapHost
    Display    = @%systemroot%\system32\eapsvc.dll,-1
    ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type       = Share_Process
    Start      = Manual
    Group      =

Mon Apr 18 16:26:07 2016Z
    Name       = MSKSSRV
    Display    = Microsoft Streaming Service Proxy
    ImagePath = system32\drivers\MSKSSRV.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = Extended Base

Mon Apr 18 16:17:34 2016Z
    Name       = ipsec
    Display    =
    ImagePath =
    Type       =
    Start      =
    Group      =

Mon Apr 18 16:17:30 2016Z
    Name       = Browser
    Display    = Computer Browser
    ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type       = Share_Process
    Start      = Disabled
    Group      = NetworkProvider

    Name       = HomeGroupListener
```

Page 80

```
                              SYSTEM OUTPUT.txt
 Display      = HomeGroup Listener
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
 Type         = Share_Process
 Start        = Disabled
 Group        =

 Name         = HomeGroupProvider
 Display      = HomeGroup Provider
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
 Type         = Share_Process
 Start        = Disabled
 Group        =

 Name         = WPCSvc
 Display      = Parental Controls
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
 Type         = Share_Process
 Start        = Disabled
 Group        =

Mon Apr 18 16:03:47 2016Z
 Name         = HipShieldK
 Display      = McAfee Inc. HipShieldK
 ImagePath = system32\drivers\HipShieldK.sys
 Type         = Kernel driver
 Start        = Manual
 Group        =

Mon Apr 18 16:02:36 2016Z
 Name         = HipMgmt
 Display      = McAfee Host Intrusion Prevention lpc Service
 ImagePath = "C:\Program Files (x86)\McAfee\Host Intrusion Prevention\HipMgmt.exe"
 Type         = Own_Process
 Start        = Auto Start
 Group        =

Mon Apr 18 16:02:15 2016Z
 Name         = FireNfcp
 Display      = McAfee Inc. FireNfcp
 ImagePath = system32\drivers\FireNfcp.sys
 Type         = Kernel driver
 Start        = Manual
 Group        =

Mon Apr 18 15:58:37 2016Z
 Name         = McTaskManager
 Display      = McAfee Task Manager
 ImagePath = "C:\Program Files (x86)\McAfee\VirusScan Enterprise\VsTskMgr.exe"
 Type         = Own_Process
 Start        = Auto Start
 Group        =

Mon Apr 18 15:58:26 2016Z
 Name         = SNMP
 Display      =
 ImagePath =
 Type         =
 Start        =
 Group        =

Mon Apr 18 15:57:48 2016Z
 Name         = PCP
 Display      =
```

Page 81

SYSTEM OUTPUT.txt

```
ImagePath =
Type      =
Start     =
Group     = NetworkProvider

Mon Apr 18 15:57:46 2016Z
Name      = eventlog
Display   = @%SystemRoot%\system32\wevtsvc.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     = Event Log

Name      = Pointsec
Display   = Pointsec
ImagePath = C:\WINDOWS\SysWOW64\Prot_srv.exe
Type      = 0x0
Start     = Auto Start
Group     = PlugPlay

Name      = Pointsec_Start
Display   = Pointsec Service Start
ImagePath = C:\WINDOWS\SysWOW64\PstartSr.exe
Type      = 0x0
Start     = Auto Start
Group     =

Mon Apr 18 15:57:14 2016Z
Name      = CVPND
Display   = Cisco Systems, Inc. VPN Service
ImagePath = "C:\Program Files (x86)\Cisco Systems\VPN Client\cvpnd.exe"
Type      = 0x0
Start     = Auto Start
Group     =

Mon Apr 18 15:57:04 2016Z
Name      = {2A088A0C-A99B-4B11-81C8-178260EEB892}
Display   =
ImagePath =
Type      =
Start     =
Group     =

Mon Apr 18 15:56:53 2016Z
Name      = {915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3}
Display   =
ImagePath =
Type      =
Start     =
Group     =

Mon Apr 18 15:56:52 2016Z
Name      = vpnagent
Display   = Cisco AnyConnect Secure Mobility Agent
ImagePath = "C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\vpnagent.exe"
Type      = Own_Process
Start     = Auto Start
Group     = TDI

Mon Apr 18 15:54:46 2016Z
Name      = atashost
Display   = WebEx Service Host for Support Center
```

Page 82

```
                          SYSTEM OUTPUT.txt
    ImagePath = "C:\WINDOWS\SysWOW64\atashost.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Mon Apr 18 15:54:18 2016Z
    Name      = enstart64
    Display   = enstart64
    ImagePath = C:\WINDOWS\system32\enstart64.exe
    Type      = Own_Process
    Start     = Auto Start
    Group     =

Mon Apr 18 15:50:45 2016Z
    Name      = IEEtwCollectorService
    Display   = @%SystemRoot%\system32\ieetwcollectorres.dll,-1000
    ImagePath = %SystemRoot%\system32\IEEtwCollector.exe /V
    Type      = Own_Process
    Start     = Manual
    Group     =

Mon Apr 18 15:48:25 2016Z
    Name      = MSDTC Bridge 4.0.0.0
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =

    Name      = SMSvcHost 4.0.0.0
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =

    Name      = Windows Workflow Foundation 4.0.0.0
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =

Mon Apr 18 15:45:34 2016Z
    Name      = ac.sharedstore
    Display   = ActivIdentity Shared Store Service
    ImagePath = "C:\Program Files\Common Files\ActivIdentity\ac.sharedstore.exe"
    Type      = Own_Process
    Start     = Auto Start
    Group     = SmartCardGroup

Mon Apr 18 15:45:08 2016Z
    Name      = AdobeFlashPlayerUpdateSvc
    Display   = Adobe Flash Player Update Service
    ImagePath = C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
    Type      = Own_Process
    Start     = Manual
    Group     =

Mon Apr 18 15:44:49 2016Z
    Name      = AdobeARMservice
    Display   = Adobe Acrobat Update Service
    ImagePath = "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
                          Page 83
```

SYSTEM OUTPUT.txt
```
    Type       = Own_Process
    Start      = Auto Start
    Group      =

Mon Apr 18 15:43:23 2016Z
    Name       = ASP.NET_4.0.30319
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

Mon Apr 18 15:43:21 2016Z
    Name       = ASP.NET
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

Mon Apr 18 15:43:18 2016Z
    Name       = aspnet_state
    Display    = ASP.NET State Service
    ImagePath  = %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
    Type       = Own_Process
    Start      = Manual
    Group      =

Mon Apr 18 15:43:15 2016Z
    Name       = .NET Memory Cache 4.0
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = NetMsmqActivator
    Display    =
@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8195
    ImagePath  = "C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"
-NetMsmqActivator
    Type       = Share_Process
    Start      = Disabled
    Group      =

    Name       = NetPipeActivator
    Display    =
@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8197
    ImagePath  = C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
    Type       = Share_Process
    Start      = Disabled
    Group      =

    Name       = NetTcpActivator
    Display    =
@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8199
    ImagePath  = C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
    Type       = Share_Process
    Start      = Disabled
    Group      =

    Name       = NetTcpPortSharing
    Display    =
```

Page 84

```
                              SYSTEM OUTPUT.txt
@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8201
    ImagePath = C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
    Type      = Share_Process
    Start     = Disabled
    Group     =


Mon Apr 18 15:42:19 2016Z
    Name      = clr_optimization_v4.0.30319_32
    Display   = Microsoft .NET Framework NGEN v4.0.30319_X86
    ImagePath = C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
    Type      = Own_Process
    Start     = Auto Start
    Group     =


    Name      = clr_optimization_v4.0.30319_64
    Display   = Microsoft .NET Framework NGEN v4.0.30319_X64
    ImagePath = C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
    Type      = Own_Process
    Start     = Auto Start
    Group     =


Mon Apr 18 15:42:14 2016Z
    Name      = .NET CLR Networking 4.0.0.0
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =


Mon Apr 18 15:42:12 2016Z
    Name      = clr_optimization_v2.0.50727_32
    Display   = Microsoft .NET Framework NGEN v2.0.50727_X86
    ImagePath = %systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
    Type      = Own_Process
    Start     = Disabled
    Group     =


    Name      = clr_optimization_v2.0.50727_64
    Display   = Microsoft .NET Framework NGEN v2.0.50727_X64
    ImagePath = %systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
    Type      = Own_Process
    Start     = Disabled
    Group     =


Mon Apr 18 15:37:48 2016Z
    Name      = dcdbas
    Display   = System Management Driver
    ImagePath = system32\DRIVERS\dcdbas64.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =


Mon Apr 18 15:34:47 2016Z
    Name      = BthEnum
    Display   = Bluetooth Enumerator Service
    ImagePath = system32\DRIVERS\BthEnum.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =


    Name      = BthPan
    Display   = Bluetooth Device (Personal Area Network)
    ImagePath = system32\DRIVERS\bthpan.sys
                              Page 85
```

SYSTEM OUTPUT.txt

```
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Name        = RFCOMM
Display     = Bluetooth Device (RFCOMM Protocol TDI)
ImagePath   = system32\DRIVERS\rfcomm.sys
Type        = Kernel driver
Start       = Manual
Group       = PNP_TDI
```

Mon Apr 18 15:34:46 2016Z
```
Name        = BTHUSB
Display     = Bluetooth Radio USB Driver
ImagePath   = System32\Drivers\BTHUSB.sys
Type        = Kernel driver
Start       = Manual
Group       = PNP Filter
```

Mon Apr 18 15:31:22 2016Z
```
Name        = CcmExec
Display     = SMS Agent Host
ImagePath   = C:\WINDOWS\CCM\CcmExec.exe
Type        = Own_Process
Start       = Auto Start
Group       =

Name        = smstsmgr
Display     = ConfigMgr Task Sequence Agent
ImagePath   = C:\WINDOWS\CCM\TSManager.exe /service
Type        = Own_Process
Start       = Manual
Group       =
```

Mon Apr 18 15:30:46 2016Z
```
Name        = lpasvc
Display     = Microsoft Policy Platform Local Authority
ImagePath   = "C:\Program Files\Microsoft Policy Platform\policyHost.exe" /service
Type        = Share_Process
Start       = Manual
Group       =

Name        = lppsvc
Display     = Microsoft Policy Platform Processor
ImagePath   = "C:\Program Files\Microsoft Policy Platform\policyHost.exe" /service
Type        = Share_Process
Start       = Manual
Group       =
```

Mon Apr 18 15:30:13 2016Z
```
Name        = Netlogon
Display     = @%SystemRoot%\System32\netlogon.dll,-102
ImagePath   = %systemroot%\system32\lsass.exe
Type        = Share_Process
Start       = Auto Start
Group       = MS_WindowsRemoteValidation
```

Mon Apr 18 15:30:12 2016Z
```
Name        = cphs
Display     = Intel(R) Content Protection HECI Service
ImagePath   = %SystemRoot%\SysWow64\IntelCpHeciSvc.exe
Type        = Own_Process
Start       = Manual
```

Page 86

```
                          SYSTEM OUTPUT.txt
    Group       =

    Name        = IKEEXT
    Display     = @%SystemRoot%\system32\ikeext.dll,-501
    ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

Mon Apr 18 15:29:32 2016Z
    Name        = TabletInputService
    Display     = @%SystemRoot%\system32\TabSvc.dll,-100
    ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
    Type        = Share_Process
    Start       = Auto Start
    Group       = PlugPlay

Mon Apr 18 15:29:01 2016Z
    Name        = WinDefend
    Display     = @%ProgramFiles%\Windows Defender\MsMpRes.dll,-103
    ImagePath   = %SystemRoot%\System32\svchost.exe -k secsvcs
    Type        = Share_Process
    Start       = Manual
    Group       =

Mon Apr 18 15:28:58 2016Z
    Name        = {4525A64F-379A-4D68-8A81-DA5AA833E191}
    Display     =
    ImagePath   =
    Type        =
    Start       =
    Group       =

Mon Apr 18 15:28:54 2016Z
    Name        = CertPropSvc
    Display     = @%SystemRoot%\System32\certprop.dll,-11
    ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

    Name        = SCardSvr
    Display     = @%SystemRoot%\System32\SCardSvr.dll,-1
    ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
    Type        = Share_Process
    Start       = Auto Start
    Group       = SmartCardGroup

Mon Apr 18 15:28:51 2016Z
    Name        = BTHPORT
    Display     = Bluetooth Port Driver
    ImagePath   = System32\Drivers\BTHport.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = PNP Filter

Mon Apr 18 15:28:13 2016Z
    Name        = MSPQM
    Display     = Microsoft Streaming Quality Manager Proxy
    ImagePath   = system32\drivers\MSPQM.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = Extended Base
                          Page 87
```

SYSTEM OUTPUT.txt

```
Name      = MSTEE
Display   = Microsoft Streaming Tee/Sink-to-Sink Converter
ImagePath = system32\drivers\MSTEE.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Mon Apr 18 15:28:12 2016Z
Name      = MSPCLOCK
Display   = Microsoft Streaming Clock Proxy
ImagePath = system32\drivers\MSPCLOCK.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Mon Apr 18 15:28:07 2016Z
Name      = RtkAudioService
Display   = Realtek Audio Service
ImagePath = "C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe"
Type      = Own_Process
Start     = Auto Start
Group     = PlugPlay

Mon Apr 18 15:28:04 2016Z
Name      = Wlansvc
Display   = @%SystemRoot%\System32\wlansvc.dll,-257
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     = TDI

Mon Apr 18 15:28:03 2016Z
Name      = {033026B9-7329-415D-8068-DD988B393525}
Display   =
ImagePath =
Type      =
Start     =
Group     =

Mon Apr 18 15:28:02 2016Z
Name      = O2FLASH
Display   = O2FLASH
ImagePath = %SystemRoot%\system32\DRIVERS\o2flash.exe
Type      = Own_Process
Start     = Auto Start
Group     =

Mon Apr 18 15:28:01 2016Z
Name      = nvsvc
Display   = NVIDIA Display Driver Service
ImagePath = "C:\WINDOWS\system32\nvvsvc.exe"
Type      = Own_Process
Start     = Auto Start
Group     = Video

Mon Apr 18 15:27:42 2016Z
Name      = ApHidMonitorService
Display   = Alps HID Monitor Service
ImagePath = C:\Program Files\DellTPad\HidMonitorSvc.exe
Type      = Own_Process
Start     = Auto Start
Group     =
```

Page 88

SYSTEM OUTPUT.txt

```
Mon Apr 18 15:27:40 2016Z
    Name      = {4BA4B36E-29B2-45EB-8693-07A52C8F3CC5}
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =

Mon Apr 18 15:27:22 2016Z
    Name      = ialm
    Display   =
    ImagePath =
    Type      =
    Start     =
    Group     =

Mon Apr 18 15:27:21 2016Z
    Name      = igfxCUIService1.0.0.0
    Display   = Intel(R) HD Graphics Control Panel Service
    ImagePath = %SystemRoot%\system32\igfxCUIService.exe
    Type      = Own_Process
    Start     = Auto Start
    Group     = ProfSvc_Group

Mon Apr 18 15:26:58 2016Z
    Name      = atapi
    Display   =
    ImagePath = \SystemRoot\system32\drivers\atapi.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = SCSI Miniport

    Name      = cdrom
    Display   =
    ImagePath = \SystemRoot\system32\drivers\cdrom.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = SCSI CDROM Class

    Name      = HpSAMD
    Display   =
    ImagePath = \SystemRoot\system32\drivers\HpSAMD.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = SCSI Miniport

    Name      = isapnp
    Display   =
    ImagePath = \SystemRoot\system32\drivers\isapnp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Boot Bus Extender

    Name      = LSI_SAS
    Display   =
    ImagePath = \SystemRoot\system32\drivers\lsi_sas.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = SCSI Miniport

    Name      = LSI_SCSI
    Display   =
```

Page 89

```
                              SYSTEM OUTPUT.txt
ImagePath = \SystemRoot\system32\drivers\lsi_scsi.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = MegaSR
Display   =
ImagePath = \SystemRoot\system32\drivers\MegaSR.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = msahci
Display   =
ImagePath = \SystemRoot\system32\drivers\msahci.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = nvraid
Display   =
ImagePath = \SystemRoot\system32\drivers\nvraid.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Name      = pciide
Display   =
ImagePath = \SystemRoot\system32\drivers\pciide.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Name      = sbp2port
Display   =
ImagePath = \SystemRoot\system32\drivers\sbp2port.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = wd
Display   =
ImagePath = \SystemRoot\system32\drivers\wd.sys
Type      = Kernel driver
Start     = Manual
Group     =

Mon Apr 18 15:26:57 2016Z
Name      = adp94xx
Display   =
ImagePath = \SystemRoot\system32\drivers\adp94xx.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = adpahci
Display   =
ImagePath = \SystemRoot\system32\drivers\adpahci.sys
Type      = Kernel driver
Start     = Manual
Group     = SCSI Miniport

Name      = adpu320
```

Page 90

SYSTEM OUTPUT.txt
```
Display     =
ImagePath = \SystemRoot\system32\drivers\adpu320.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = aliide
Display     =
ImagePath = \SystemRoot\system32\drivers\aliide.sys
Type        = Kernel driver
Start       = Manual
Group       = System Bus Extender

Name        = amdide
Display     =
ImagePath = \SystemRoot\system32\drivers\amdide.sys
Type        = Kernel driver
Start       = Manual
Group       = System Bus Extender

Name        = amdsata
Display     =
ImagePath = \SystemRoot\system32\drivers\amdsata.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI miniport

Name        = amdsbs
Display     =
ImagePath = \SystemRoot\system32\drivers\amdsbs.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = arc
Display     =
ImagePath = \SystemRoot\system32\drivers\arc.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = arcsas
Display     =
ImagePath = \SystemRoot\system32\drivers\arcsas.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI miniport

Name        = cmdide
Display     =
ImagePath = \SystemRoot\system32\drivers\cmdide.sys
Type        = Kernel driver
Start       = Manual
Group       = System Bus Extender

Name        = elxstor
Display     =
ImagePath = \SystemRoot\system32\drivers\elxstor.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = iaStorV
```
Page 91

SYSTEM OUTPUT.txt
```
Display     =
ImagePath   = \SystemRoot\system32\drivers\iaStorV.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = iirsp
Display     =
ImagePath   = \SystemRoot\system32\drivers\iirsp.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = intelide
Display     =
ImagePath   = \SystemRoot\system32\drivers\intelide.sys
Type        = Kernel driver
Start       = Manual
Group       = System Bus Extender

Name        = LSI_FC
Display     =
ImagePath   = \SystemRoot\system32\drivers\lsi_fc.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = LSI_SAS2
Display     =
ImagePath   = \SystemRoot\system32\drivers\lsi_sas2.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = megasas
Display     =
ImagePath   = \SystemRoot\system32\drivers\megasas.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = mpio
Display     =
ImagePath   = \SystemRoot\system32\drivers\mpio.sys
Type        = Kernel driver
Start       = Manual
Group       = Boot Bus Extender

Name        = msdsm
Display     =
ImagePath   = \SystemRoot\system32\drivers\msdsm.sys
Type        = Kernel driver
Start       = Manual
Group       = System Bus Extender

Name        = nfrd960
Display     =
ImagePath   = \SystemRoot\system32\drivers\nfrd960.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI Miniport

Name        = nvstor
```
Page 92

SYSTEM OUTPUT.txt

```
Display    =
ImagePath = \SystemRoot\system32\drivers\nvstor.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = ql2300
Display    =
ImagePath = \SystemRoot\system32\drivers\ql2300.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = ql40xx
Display    =
ImagePath = \SystemRoot\system32\drivers\ql40xx.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = SiSRaid2
Display    =
ImagePath = \SystemRoot\system32\drivers\SiSRaid2.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = SiSRaid4
Display    =
ImagePath = \SystemRoot\system32\drivers\sisraid4.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = ST7007
Display    =
ImagePath = \SystemRoot\system32\drivers\ST7007.sys
Type       = Kernel driver
Start      = Manual
Group      = System Bus Extender

Name       = stexstor
Display    =
ImagePath = \SystemRoot\system32\drivers\stexstor.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Name       = storvsc
Display    =
ImagePath = \SystemRoot\system32\drivers\storvsc.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Name       = viaide
Display    =
ImagePath = \SystemRoot\system32\drivers\viaide.sys
Type       = Kernel driver
Start      = Manual
Group      = System Bus Extender

Name       = vsmraid
```

Page 93

SYSTEM OUTPUT.txt

```
Display    =
ImagePath = \SystemRoot\system32\drivers\vsmraid.sys
Type       = Kernel driver
Start      = Manual
Group      = SCSI Miniport

Mon Apr 18 15:26:55 2016Z
Name       = TsUsbGD
Display    = Remote Desktop Generic USB Device
ImagePath = \SystemRoot\system32\drivers\TsUsbGD.sys
Type       = Kernel driver
Start      = Manual
Group      = Extended Base

Mon Apr 18 15:24:49 2016Z
Name       = bcmnfcusb
Display    = NFC USB Bus Driver
ImagePath = \SystemRoot\system32\drivers\bcmnfcusb7.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Mon Apr 18 15:23:49 2016Z
Name       = ISCT
Display    = Intel(R) Smart Connect Technology Device Driver
ImagePath = \SystemRoot\system32\drivers\ISCTD.sys
Type       = Kernel driver
Start      = Manual
Group      = Extended Base

Mon Apr 18 15:22:46 2016Z
Name       = iwsehub
Display    = Intel(R) WSE Hub Driver
ImagePath = \SystemRoot\system32\drivers\iwsehub.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Name       = iwsepal
Display    = Intel(R) WSE-PAL Driver
ImagePath = \SystemRoot\system32\drivers\iwsepal.sys
Type       = Kernel driver
Start      = Manual
Group      = Base

Mon Apr 18 15:22:43 2016Z
Name       = swmbbnmea05
Display    = Sierra Wireless USB Device for NMEA Serial Communication - Dell
ImagePath = \SystemRoot\system32\drivers\swmbbnmea05.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = swmbbser05
Display    = Sierra Wireless USB Device for Serial Communication - Dell
ImagePath = \SystemRoot\system32\drivers\swmbbser05.sys
Type       = Kernel driver
Start      = Manual
Group      =

Mon Apr 18 15:22:42 2016Z
Name       = swg3knmea05
Display    = Sierra Wireless QMI NMEA Communication - Dell
```

Page 94

SYSTEM OUTPUT.txt
```
ImagePath = \SystemRoot\system32\drivers\swg3knmea05.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = swg3kser05
Display   = Sierra Wireless QMI USB Device for Legacy Serial Communication - Dell
ImagePath = \SystemRoot\system32\drivers\swg3kser05.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = swibus05
Display   = Sierra Wireless Bus Enumerator 05
ImagePath = \SystemRoot\system32\drivers\swibus05.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Name      = swibusflt05
Display   = Sierra Wireless Bus Enumerator Filter 05
ImagePath = \SystemRoot\system32\drivers\swibusflt05.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = swimbbbus05
Display   = Sierra Wireless MBB Device Bus Enumerator 05
ImagePath = \SystemRoot\system32\drivers\swimbbbus05.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Name      = swimbbbusflt05
Display   = Sierra Wireless MBB Device Bus Enumerator Filter 05
ImagePath = \SystemRoot\system32\drivers\swimbbbusflt05.sys
Type      = Kernel driver
Start     = Manual
Group     =

Wed Dec 30 14:09:15 2015Z
Name      = VMBusHID
Display   =
ImagePath = \SystemRoot\system32\drivers\VMBusHID.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Wed Dec 30 14:08:57 2015Z
Name      = tsusbhub
Display   = Remote Deskotop USB Hub
ImagePath = \SystemRoot\system32\drivers\tsusbhub.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Wed Dec 30 14:08:56 2015Z
Name      = fdc
Display   = Floppy Disk Controller Driver
ImagePath = \SystemRoot\system32\drivers\fdc.sys
Type      = Kernel driver
Start     = Manual
Group     =
```

Page 95

SYSTEM OUTPUT.txt

```
Wed Dec 30 14:08:48 2015Z
  Name      = flpydisk
  Display   = Floppy Disk Driver
  ImagePath = \SystemRoot\system32\drivers\flpydisk.sys
  Type      = Kernel driver
  Start     = Manual
  Group     =

Wed Dec 30 14:08:47 2015Z
  Name      = Synth3dVsc
  Display   = Microsoft Virtual 3D Video Transport Driver
  ImagePath = \SystemRoot\system32\drivers\Synth3dVsc.sys
  Type      = Kernel driver
  Start     = Manual
  Group     = Extended Base

Wed Dec 30 14:08:18 2015Z
  Name      = s3cap
  Display   =
  ImagePath = \SystemRoot\system32\drivers\vms3cap.sys
  Type      = Kernel driver
  Start     = Manual
  Group     = Video

Wed Dec 30 14:05:27 2015Z
  Name      = WSearch
  Display   = @%systemroot%\system32\SearchIndexer.exe,-103
  ImagePath = %systemroot%\system32\SearchIndexer.exe /Embedding
  Type      = Own_Process
  Start     = Auto Start
  Group     =

Wed Dec 30 14:05:22 2015Z
  Name      = FDResPub
  Display   = @%systemroot%\system32\fdrespub.dll,-100
  ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
  Type      = Share_Process
  Start     = Manual
  Group     =

Wed Dec 30 13:52:01 2015Z
  Name      = netvsc
  Display   =
  ImagePath = system32\DRIVERS\netvsc60.sys
  Type      = Kernel driver
  Start     = Manual
  Group     = Extended Base

  Name      = SynthVid
  Display   =
  ImagePath = system32\DRIVERS\VMBusVideoM.sys
  Type      = Kernel driver
  Start     = Manual
  Group     = Video

Wed Dec 30 13:52:00 2015Z
  Name      = secdrv
  Display   = Security Driver
  ImagePath =
  Type      = Kernel driver
  Start     = Disabled
  Group     =
```

Page 96

SYSTEM OUTPUT.txt

```
    Name      = udfs
    Display   = udfs
    ImagePath = system32\DRIVERS\udfs.sys
    Type      = File system driver
    Start     = Disabled
    Group     = Boot File System

Wed Dec 30 12:33:10 2015Z
    Name      = BITS
    Display   = @%SystemRoot%\system32\qmgr.dll,-1000
    ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type      = Share_Process
    Start     = Auto Start
    Group     =

Wed Dec 30 12:27:20 2015Z
    Name      = RemoteRegistry
    Display   = @regsvc.dll,-1
    ImagePath = %SystemRoot%\system32\svchost.exe -k regsvc
    Type      = Share_Process
    Start     = Auto Start
    Group     =

Wed Dec 30 12:27:10 2015Z
    Name      = bthserv
    Display   = @%SystemRoot%\System32\bthserv.dll,-101
    ImagePath = %SystemRoot%\system32\svchost.exe -k bthsvcs
    Type      = Share_Process
    Start     = Disabled
    Group     =

Wed Dec 30 12:26:59 2015Z
    Name      = BDESVC
    Display   = @%SystemRoot%\system32\bdesvc.dll,-100
    ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type      = Share_Process
    Start     = Disabled
    Group     =

Wed Dec 30 10:09:44 2015Z
    Name      = amdxata
    Display   =
    ImagePath = system32\drivers\amdxata.sys
    Type      = Kernel driver
    Start     = Boot Start
    Group     = SCSI miniport

Wed Dec 30 09:12:34 2015Z
    Name      = WbioSrvc
    Display   = @%systemroot%\system32\wbiosrvc.dll,-100
    ImagePath = %SystemRoot%\system32\svchost.exe -k WbioSvcGroup
    Type      = Share_Process
    Start     = Manual
    Group     = SmartCardGroup

Wed Dec 30 07:48:59 2015Z
    Name      = gpsvc
    Display   = @gpapi.dll,-112
    ImagePath = %windir%\system32\svchost.exe -k GPSvcGroup
    Type      = Own_Process
    Start     = Auto Start
    Group     = ProfSvc_Group
```

Page 97

SYSTEM OUTPUT.txt

```
Wed Dec 30 07:41:07 2015Z
    Name        = DiagTrack
    Display     = @%SystemRoot%\system32\UtcResources.dll,-3001
    ImagePath = %SystemRoot%\System32\svchost.exe -k utcsvc
    Type        = Own_Process
    Start       = Auto Start
    Group       =

    Name        = FontCache
    Display     = @%systemroot%\system32\FntCache.dll,-100
    ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService
    Type        = Share_Process
    Start       = Auto Start
    Group       = AudioGroup

    Name        = iScsiPrt
    Display     = iScsiPort Driver
    ImagePath = \SystemRoot\system32\drivers\msiscsi.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

    Name        = terminpt
    Display     = Microsoft Remote Desktop Input Driver
    ImagePath = \SystemRoot\system32\drivers\terminpt.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = Extended Base

    Name        = usbcir
    Display     = eHome Infrared Receiver (USBCIR)
    ImagePath = \SystemRoot\system32\drivers\usbcir.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = Extended Base

    Name        = WatAdminSvc
    Display     = @%SystemRoot%\system32\Wat\WatUX.exe,-601
    ImagePath = %SystemRoot%\system32\Wat\WatAdminSvc.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

    Name        = WebClient
    Display     = @%systemroot%\system32\webclnt.dll,-100
    ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService
    Type        = Share_Process
    Start       = Manual
    Group       = NetworkProvider

    Name        = wudfsvc
    Display     = @%SystemRoot%\system32\wudfsvc.dll,-1000
    ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
    Type        = Share_Process
    Start       = Manual
    Group       = PlugPlay

Wed Dec 30 07:03:57 2015Z
    Name        = MSDTC Bridge 3.0.0.0
    Display     =
    ImagePath =
    Type        =
```

Page 98

SYSTEM OUTPUT.txt

```
Start      =
Group      =

Name       = ServiceModelEndpoint 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = ServiceModelOperation 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = ServiceModelService 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = SMSvcHost 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = Windows Workflow Foundation 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Tue Dec 29 15:55:14 2015Z
Name       = Microsoft SharePoint Workspace Audit Service
Display    = Microsoft SharePoint Workspace Audit Service
ImagePath  = "C:\Program Files (x86)\Microsoft Office\Office14\GROOVE.EXE"
/auditservice
Type       = Own_Process
Start      = Manual
Group      =

Tue Dec 29 15:55:13 2015Z
Name       = Outlook
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Tue Dec 29 15:55:12 2015Z
Name       = adsi
Display    =
ImagePath  =
Type       =
Start      =
Group      =
```

Page 99

```
                          SYSTEM OUTPUT.txt
Tue Dec 29 15:52:10 2015Z
   Name        = osppsvc
   Display     = Office Software Protection Platform
   ImagePath = "C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE"
   Type        = Own_Process
   Start       = Manual
   Group       =

Tue Dec 29 15:51:22 2015Z
   Name        = wuauserv
   Display     = @%systemroot%\system32\wuaueng.dll,-105
   ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
   Type        = Share_Process
   Start       = Auto Start
   Group       =

Tue Dec 29 15:51:11 2015Z
   Name        = ose
   Display     = Office  Source Engine
   ImagePath = "C:\Program Files (x86)\Common Files\Microsoft Shared\Source
Engine\OSE.EXE"
   Type        = Own_Process
   Start       = Manual
   Group       =

Tue Apr 12 07:45:41 2011Z
   Name        = CscService
   Display     = @%systemroot%\system32\cscsvc.dll,-200
   ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
   Type        = Share_Process
   Start       = Auto Start
   Group       = ProfSvc_Group

Tue Apr 12 07:45:24 2011Z
   Name        = AppMgmt
   Display     = @appmgmts.dll,-3250
   ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = PeerDistSvc
   Display     = @%SystemRoot%\system32\peerdistsvc.dll,-9000
   ImagePath = %SystemRoot%\System32\svchost.exe -k PeerDist
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = RdpVideoMiniport
   Display     = Remote Desktop Video Miniport Driver
   ImagePath = System32\drivers\rdpvideominiport.sys
   Type        = Kernel driver
   Start       = Manual
   Group       =

   Name        = SensrSvc
   Display     = @%SystemRoot%\System32\sensrsvc.dll,-1000
   ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
   Type        = Share_Process
   Start       = Manual
   Group       =
```

Page 100

SYSTEM OUTPUT.txt
```
Name      = StorSvc
Display   = @%SystemRoot%\System32\StorSvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = UmRdpService
Display   = @%SystemRoot%\system32\umrdp.dll,-1000
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = VGPU
Display   =
ImagePath = System32\drivers\rdvgkmd.sys
Type      = Kernel driver
Start     = Manual
Group     =

Tue Apr 12 07:45:22 2011Z
Name      = RDPUDD
Display   =
ImagePath =
Type      =
Start     =
Group     =

Tue Apr 12 07:44:54 2011Z
Name      = dmvsc
Display   =
ImagePath = \SystemRoot\system32\drivers\dmvsc.sys
Type      = Kernel driver
Start     = Manual
Group     =

Sun Nov 21 03:58:24 2010Z
Name      = BTHMODEM
Display   = Bluetooth Serial Communications Driver
ImagePath = \SystemRoot\system32\drivers\bthmodem.sys
Type      = Kernel driver
Start     = Manual
Group     =

Sun Nov 21 03:58:22 2010Z
Name      = gagp30kx
Display   = Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms
ImagePath = \SystemRoot\system32\drivers\gagp30kx.sys
Type      = Kernel driver
Start     = Manual
Group     = PnP Filter

Name      = uagp35
Display   = Microsoft AGPv3.5 Filter
ImagePath = \SystemRoot\system32\drivers\uagp35.sys
Type      = Kernel driver
Start     = Manual
Group     = PnP Filter

Sun Nov 21 03:58:21 2010Z
Name      = b06bdrv
Display   = Broadcom NetXtreme II VBD
```

Page 101

```
                               SYSTEM OUTPUT.txt
ImagePath = \SystemRoot\system32\drivers\bxvbda.sys
Type      = Kernel driver
Start     = Manual
Group     = base

Name      = HidBth
Display   = Microsoft Bluetooth HID Miniport
ImagePath = \SystemRoot\system32\drivers\hidbth.sys
Type      = Kernel driver
Start     = Manual
Group     = extended base

Sun Nov 21 03:58:19 2010Z
Name      = AmdK8
Display   = AMD K8 Processor Driver
ImagePath = \SystemRoot\system32\drivers\amdk8.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Name      = AmdPPM
Display   = AMD Processor Driver
ImagePath = \SystemRoot\system32\drivers\amdppm.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Name      = Processor
Display   = Processor Driver
ImagePath = \SystemRoot\system32\drivers\processr.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Sun Nov 21 03:58:18 2010Z
Name      = ebdrv
Display   = Broadcom NetXtreme II 10 GigE VBD
ImagePath = \SystemRoot\system32\drivers\evbda.sys
Type      = Kernel driver
Start     = Manual
Group     = base

Sun Nov 21 03:58:17 2010Z
Name      = pcmcia
Display   =
ImagePath = \SystemRoot\system32\drivers\pcmcia.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Sun Nov 21 03:58:16 2010Z
Name      = MTConfig
Display   = Microsoft Input Configuration Driver
ImagePath = \SystemRoot\system32\drivers\MTConfig.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Sun Nov 21 03:58:15 2010Z
Name      = circlass
Display   = Consumer IR Devices
ImagePath = \SystemRoot\system32\drivers\circlass.sys
Type      = Kernel driver
```

Page 102

SYSTEM OUTPUT.txt

```
    Start       = Manual
    Group    .  = Extended Base

Sun Nov 21 03:58:13 2010Z
    Name        = sfloppy
    Display     = High-Capacity Floppy Disk Drive
    ImagePath = \SystemRoot\system32\drivers\sfloppy.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

Sun Nov 21 03:58:11 2010Z
    Name        = HidBatt
    Display     = HID UPS Battery Driver
    ImagePath = \SystemRoot\system32\drivers\HidBatt.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

Sun Nov 21 03:58:08 2010Z
    Name        = HidIr
    Display     = Microsoft Infrared HID Driver
    ImagePath = \SystemRoot\system32\drivers\hidir.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = extended base

Sun Nov 21 03:58:07 2010Z
    Name        = sermouse
    Display     = Serial Mouse Driver
    ImagePath = \SystemRoot\system32\drivers\sermouse.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = Pointer Port

Sun Nov 21 03:58:06 2010Z
    Name        = BrFiltLo
    Display     = Brother USB Mass-Storage Lower Filter Driver
    ImagePath = \SystemRoot\system32\drivers\BrFiltLo.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = extended base

    Name        = BrFiltUp
    Display     = Brother USB Mass-Storage Upper Filter Driver
    ImagePath = \SystemRoot\system32\drivers\BrFiltUp.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = extended base

Sun Nov 21 03:58:05 2010Z
    Name        = usbohci
    Display     = Microsoft USB Open Host Controller Miniport Driver
    ImagePath = \SystemRoot\system32\drivers\usbohci.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = Base

    Name        = usbuhci
    Display     = Microsoft USB Universal Host Controller Miniport Driver
    ImagePath = \SystemRoot\system32\drivers\usbuhci.sys
    Type        = Kernel driver
    Start       = Manual
```

Page 103

```
                          SYSTEM OUTPUT.txt
    Group      = Base

Sun Nov 21 03:58:00 2010Z
    Name       = WacomPen
    Display    = Wacom Serial Pen HID Driver
    ImagePath = \SystemRoot\system32\drivers\wacompen.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = Extended Base

Sun Nov 21 03:57:59 2010Z
    Name       = crcdisk
    Display    = Crcdisk Filter Driver
    ImagePath = \SystemRoot\system32\drivers\crcdisk.sys
    Type       = Kernel driver
    Start      = Disabled
    Group      = Pnp Filter

Sun Nov 21 03:57:58 2010Z
    Name       = UmPass
    Display    = Microsoft UMPass Driver
    ImagePath = \SystemRoot\system32\drivers\umpass.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = Extended Base

Sun Nov 21 03:57:56 2010Z
    Name       = usbprint
    Display    = Microsoft USB PRINTER Class
    ImagePath = \SystemRoot\system32\drivers\usbprint.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = extended base

Sun Nov 21 03:46:56 2010Z
    Name       = b57nd60a
    Display    = Broadcom NetXtreme Gigabit Ethernet - NDIS 6.0
    ImagePath = system32\DRIVERS\b57nd60a.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = NDIS

    Name       = cdfs
    Display    = CD/DVD File System Reader
    ImagePath = system32\DRIVERS\cdfs.sys
    Type       = File system driver
    Start      = Disabled
    Group      = Boot File System

    Name       = fastfat
    Display    = FAT12/16/32 File System Driver
    ImagePath =
    Type       = File system driver
    Start      = Manual
    Group      = Boot File System

    Name       = vga
    Display    =
    ImagePath = system32\DRIVERS\vgapnp.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = Video
```

Page 104

SYSTEM OUTPUT.txt

```
Sun Nov 21 03:38:46 2010Z
    Name      = TsUsbFlt
    Display   =
    ImagePath = system32\drivers\tsusbflt.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = base

Sun Nov 21 03:33:56 2010Z
    Name      = SessionEnv
    Display   = @%SystemRoot%\System32\SessEnv.dll,-1026
    ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type      = Share_Process
    Start     = Manual
    Group     =

Sun Nov 21 03:29:32 2010Z
    Name      = 1394ohci
    Display   = 1394 OHCI Compliant Host Controller
    ImagePath = \SystemRoot\system32\drivers\1394ohci.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = AcpiPmi
    Display   = ACPI Power Meter Driver
    ImagePath = \SystemRoot\system32\drivers\acpipmi.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = agp440
    Display   = Intel AGP Bus Filter
    ImagePath = \SystemRoot\system32\drivers\agp440.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = PnP Filter

    Name      = ErrDev
    Display   = Microsoft Hardware Error Device Driver
    ImagePath = \SystemRoot\system32\drivers\errdev.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = Extended Base

    Name      = IPMIDRV
    Display   =
    ImagePath = \SystemRoot\system32\drivers\IPMIDrv.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = nv_agp
    Display   = NVIDIA nForce AGP Bus Filter
    ImagePath = \SystemRoot\system32\drivers\nv_agp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = PnP Filter

    Name      = ohci1394
    Display   = 1394 OHCI Compliant Host Controller (Legacy)
    ImagePath = \SystemRoot\system32\drivers\ohci1394.sys
    Type      = Kernel driver
```

Page 105

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       =

Name        = sffdisk
Display     = SFF Storage Class Driver
ImagePath   = \SystemRoot\system32\drivers\sffdisk.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = sffp_mmc
Display     = SFF Storage Protocol Driver for MMC
ImagePath   = \SystemRoot\system32\drivers\sffp_mmc.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = sffp_sd
Display     = SFF Storage Protocol Driver for SDBus
ImagePath   = \SystemRoot\system32\drivers\sffp_sd.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = uliagpkx
Display     = Uli AGP Bus Filter
ImagePath   = \SystemRoot\system32\drivers\uliagpkx.sys
Type        = Kernel driver
Start       = Manual
Group       = PnP Filter

Name        = vhdmp
Display     =
ImagePath   = \SystemRoot\system32\drivers\vhdmp.sys
Type        = Kernel driver
Start       = Manual
Group       = SCSI miniport

Tue Jul 14 04:54:38 2009Z
Name        = NdisCap
Display     = NDIS Capture LightWeight Filter
ImagePath   = system32\DRIVERS\ndiscap.sys
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Tue Jul 14 04:53:57 2009Z
Name        = Smb
Display     = @%SystemRoot%\system32\tcpipcfg.dll,-50005
ImagePath   = system32\DRIVERS\smb.sys
Type        = Kernel driver
Start       = Manual
Group       = PNP_TDI

Tue Jul 14 04:53:45 2009Z
Name        = TrkWks
Display     = @%SystemRoot%\system32\trkwks.dll,-1
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Auto Start
Group       =

Tue Jul 14 04:53:36 2009Z
```

Page 106

```
                                   SYSTEM OUTPUT.txt
    Name        = RpcEptMapper
    Display     = @%windir%\system32\RpcEpMap.dll,-1001
    ImagePath = %SystemRoot%\system32\svchost.exe -k RPCSS
    Type        = Share_Process
    Start       = Auto Start
    Group       = COM Infrastructure

Tue Jul 14 04:53:33 2009Z
    Name        = LanmanServer
    Display     = @%systemroot%\system32\srvsvc.dll,-100
    ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

Tue Jul 14 04:53:31 2009Z
    Name        = LanmanWorkstation
    Display     = @%systemroot%\system32\wkssvc.dll,-100
    ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService
    Type        = Share_Process
    Start       = Auto Start
    Group       = NetworkProvider

Tue Jul 14 04:53:25 2009Z
    Name        = WmiApRpl
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

Tue Jul 14 04:53:24 2009Z
    Name        = Winmgmt
    Display     = @%Systemroot%\system32\wbem\wmisvc.dll,-205
    ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

    Name        = wmiApSrv
    Display     = @%Systemroot%\system32\wbem\wmiapsrv.exe,-110
    ImagePath = %systemroot%\system32\wbem\WmiApSrv.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

Tue Jul 14 04:53:21 2009Z
    Name        = TCPIP6
    Display     = Microsoft IPv6 Protocol Driver
    ImagePath = system32\DRIVERS\tcpip.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

    Name        = WANARP
    Display     = @%systemroot%\system32\rascfg.dll,-32011
    ImagePath = system32\DRIVERS\wanarp.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

Tue Jul 14 04:53:20 2009Z
    Name        = lmhosts
```

Page 107

```
                          SYSTEM OUTPUT.txt
Display    = @%SystemRoot%\system32\lmhsvc.dll,-101
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type       = Share_Process
Start      = Auto Start
Group      = TDI

Tue Jul 14 04:53:19 2009Z
  Name       = Dhcp
  Display    = @%SystemRoot%\system32\dhcpcore.dll,-100
  ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
  Type       = Share_Process
  Start      = Auto Start
  Group      = TDI

  Name       = Winsock
  Display    =
  ImagePath =
  Type       = 0x0
  Start      = Manual
  Group      =

Tue Jul 14 04:49:48 2009Z
  Name       = SamSs
  Display    = @%SystemRoot%\system32\samsrv.dll,-1
  ImagePath = %SystemRoot%\system32\lsass.exe
  Type       = Share_Process
  Start      = Auto Start
  Group      = MS_WindowsLocalValidation

  Name       = W32Time
  Display    = @%SystemRoot%\system32\w32time.dll,-200
  ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService
  Type       = Share_Process
  Start      = Manual
  Group      =

Tue Jul 14 04:49:46 2009Z
  Name       = Dnscache
  Display    = @%SystemRoot%\System32\dnsapi.dll,-101
  ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkService
  Type       = Share_Process
  Start      = Auto Start
  Group      = TDI

Tue Jul 14 04:49:45 2009Z
  Name       = RemoteAccess
  Display    = @%Systemroot%\system32\mprdim.dll,-200
  ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
  Type       = Share_Process
  Start      = Disabled
  Group      =

Tue Jul 14 04:49:35 2009Z
  Name       = RasAuto
  Display    = @%Systemroot%\system32\rasauto.dll,-200
  ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
  Type       = Share_Process
  Start      = Manual
  Group      =

  Name       = RasMan
  Display    = @%Systemroot%\system32\rasmans.dll,-200
  ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
                          Page 108
```

```
                            SYSTEM OUTPUT.txt
    Type       = Share_Process
    Start      = Manual
    Group      =

Tue Jul 14 04:49:24 2009Z
    Name       = DPS
    Display    = @%systemroot%\system32\dps.dll,-500
    ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork
    Type       = Share_Process
    Start      = Auto Start
    Group      =

    Name       = WdiServiceHost
    Display    = @%systemroot%\system32\wdi.dll,-502
    ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalService
    Type       = Share_Process
    Start      = Manual
    Group      =

    Name       = WdiSystemHost
    Display    = @%systemroot%\system32\wdi.dll,-500
    ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
    Type       = Share_Process
    Start      = Manual
    Group      =

Tue Jul 14 04:49:01 2009Z
    Name       = .NET CLR Data
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = .NET CLR Networking
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = .NET Data Provider for Oracle
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = .NET Data Provider for SqlServer
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = .NETFramework
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = AeLookupSvc
```

Page 109

```
                          SYSTEM OUTPUT.txt
Display      = @%SystemRoot%\system32\aelupsvc.dll,-1
ImagePath    = %systemroot%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Manual
Group        =

Name         = ALG
Display      = @%SystemRoot%\system32\Alg.exe,-112
ImagePath    = %SystemRoot%\System32\alg.exe
Type         = Own_Process
Start        = Manual
Group        =

Name         = AppID
Display      = @%systemroot%\system32\appidsvc.dll,-102
ImagePath    = \SystemRoot\system32\drivers\appid.sys
Type         = Kernel driver
Start        = Manual
Group        =

Name         = AppIDSvc
Display      = @%systemroot%\system32\appidsvc.dll,-100
ImagePath    = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type         = Share_Process
Start        = Manual
Group        = ProfSvc_Group

Name         = Appinfo
Display      = @%systemroot%\system32\appinfo.dll,-100
ImagePath    = %SystemRoot%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Manual
Group        =

Name         = AudioEndpointBuilder
Display      = @%SystemRoot%\system32\audiosrv.dll,-204
ImagePath    = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type         = Share_Process
Start        = Auto Start
Group        = AudioGroup

Name         = AudioSrv
Display      = @%SystemRoot%\system32\audiosrv.dll,-200
ImagePath    = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type         = Share_Process
Start        = Auto Start
Group        = AudioGroup

Name         = AxInstSV
Display      = @%SystemRoot%\system32\AxInstSV.dll,-103
ImagePath    = %SystemRoot%\system32\svchost.exe -k AxInstSVGroup
Type         = Share_Process
Start        = Manual
Group        =

Name         = BattC
Display      =
ImagePath    =
Type         =
Start        =
Group        =

Name         = BFE
```

Page 110

```
                              SYSTEM OUTPUT.txt
Display    = @%SystemRoot%\system32\bfe.dll,-1001
ImagePath  = %systemroot%\system32\svchost.exe -k LocalServiceNoNetwork
Type       = Share_Process
Start      = Auto Start
Group      = NetworkProvider

Name       = Brserid
Display    = Brother MFC Serial Port Interface Driver (WDM)
ImagePath  = \SystemRoot\System32\Drivers\Brserid.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = BrSerWdm
Display    = Brother WDM Serial driver
ImagePath  = \SystemRoot\System32\Drivers\BrSerWdm.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = BrUsbMdm
Display    = Brother MFC USB Fax Only Modem
ImagePath  = \SystemRoot\System32\Drivers\BrUsbMdm.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = BrUsbSer
Display    = Brother MFC USB Serial WDM Driver
ImagePath  = \SystemRoot\System32\Drivers\BrUsbSer.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = COMSysApp
Display    = @comres.dll,-947
ImagePath  = %SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
Type       = Own_Process
Start      = Manual
Group      =

Name       = crypt32
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = CryptSvc
Display    = @%SystemRoot%\system32\cryptsvc.dll,-1001
ImagePath  = %SystemRoot%\system32\svchost.exe -k NetworkService
Type       = Share_Process
Start      = Auto Start
Group      =

Name       = DCLocator
Display    =
ImagePath  =
Type       =
Start      =
Group      =
```

Page 111

```
                             SYSTEM OUTPUT.txt
Name        = DcomLaunch
Display     = @oleres.dll,-5012
ImagePath   = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type        = Share_Process
Start       = Auto Start
Group       = COM Infrastructure

Name        = defragsvc
Display     = @%SystemRoot%\system32\defragsvc.dll,-101
ImagePath   = %SystemRoot%\system32\svchost.exe -k defragsvc
Type        = Own_Process
Start       = Manual
Group       =

Name        = dot3svc
Display     = @%systemroot%\system32\dot3svc.dll,-1102
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       = TDI

Name        = EFS
Display     = @%SystemRoot%\system32\efssvc.dll,-100
ImagePath   = %SystemRoot%\System32\lsass.exe
Type        = Share_Process
Start       = Manual
Group       =

Name        = ESENT
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = EventSystem
Display     = @comres.dll,-2450
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Auto.Start
Group       =

Name        = exfat
Display     = exFAT File System Driver
ImagePath   =
Type        = File system driver
Start       = Manual
Group       = Boot File System

Name        = fdPHost
Display     = @%systemroot%\system32\fdPHost.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = Filetrace
Display     = @%SystemRoot%\system32\drivers\filetrace.sys,-10001
ImagePath   = system32\drivers\filetrace.sys
Type        = File system driver
Start       = Manual
Group       = FSFilter Activity Monitor
```

Page 112

```
                               SYSTEM OUTPUT.txt
   Name        = FontCache3.0.0.0
   Display     = @%SystemRoot%\system32\PresentationHost.exe,-3309
   ImagePath =
%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
   Type        = Own_Process
   Start       = Manual
   Group       =

   Name        = FsDepends
   Display     = @%SystemRoot%\system32\drivers\fsdepends.sys,-10001
   ImagePath = System32\drivers\FsDepends.sys
   Type        = File system driver
   Start       = Manual
   Group       = Filter

   Name        = hcw85cir
   Display     = Hauppauge Consumer Infrared Receiver
   ImagePath = \SystemRoot\system32\drivers\hcw85cir.sys
   Type        = Kernel driver
   Start       = Manual
   Group       = Extended Base

   Name        = hidserv
   Display     = @%SystemRoot%\System32\hidserv.dll,-101
   ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = hkmsvc
   Display     = @%SystemRoot%\system32\kmsvc.dll,-6
   ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = idsvc
   Display     = @%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\ServiceModelInstallRC.dll,-8193
   ImagePath = "%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\infocard.exe"
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = inetaccs
   Display     =
   ImagePath =
   Type        =
   Start       =
   Group       =

   Name        = IPBusEnum
   Display     = @%systemroot%\system32\IPBusEnum.dll,-102
   ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
   Type        = Share_Process
   Start       = Manual
   Group       =

   Name        = IpFilterDriver
   Display     = @%systemroot%\system32\rascfg.dll,-32013
   ImagePath = system32\DRIVERS\ipfltdrv.sys
   Type        = Kernel driver
                               Page 113
```

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       =

Name        = iphlpsvc
Display     = @%SystemRoot%\system32\iphlpsvc.dll,-500
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetSvcs
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = IPNAT
Display     = IP Network Address Translator
ImagePath   = System32\drivers\ipnat.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = IRENUM
Display     = @%SystemRoot%\system32\drivers\irenum.sys,-100
ImagePath   = system32\drivers\irenum.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = KeyIso
Display     = @keyiso.dll,-100
ImagePath   = %SystemRoot%\system32\lsass.exe
Type        = Share_Process
Start       = Manual
Group       =

Name        = KtmRm
Display     = @comres.dll,-2946
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = ldap
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = lltdsvc
Display     = @%SystemRoot%\system32\lltdres.dll,-1
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = Lsa
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = MMCSS
Display     = @%systemroot%\system32\mmcss.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
```

Page 114

SYSTEM OUTPUT.txt

```
Start       = Auto Start
Group       =

Name        = Modem
Display     =
ImagePath   = system32\drivers\modem.sys
Type        = Kernel driver
Start       = Manual
Group       = Extended base

Name        = MpsSvc
Display     = @%SystemRoot%\system32\FirewallAPI.dll,-23090
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork
Type        = Share_Process
Start       = Auto Start
Group       = NetworkProvider

Name        = mshidkmdf
Display     = @%SystemRoot%\system32\drivers\mshidkmdf.sys,-100
ImagePath   = \SystemRoot\System32\drivers\mshidkmdf.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Name        = MSiSCSI
Display     = @%SystemRoot%\system32\iscsidsc.dll,-5000
ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       = iSCSI

Name        = msiserver
Display     = @%SystemRoot%\system32\msimsg.dll,-27
ImagePath   = %systemroot%\system32\msiexec.exe /V
Type        = Own_Process
Start       = Manual
Group       =

Name        = MsRPC
Display     =
ImagePath   =
Type        = Kernel driver
Start       = Manual
Group       =

Name        = MSSCNTRS
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = napagent
Display     = @%SystemRoot%\system32\qagentrt.dll,-6
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =

Name        = Netman
Display     = @%SystemRoot%\system32\netman.dll,-109
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
```

Page 115

```
                         SYSTEM OUTPUT.txt
   Start      = Manual
   Group      =

   Name       = netprofm
   Display    = @%SystemRoot%\system32\netprofm.dll,-202
   ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalService
   Type       = Share_Process
   Start      = Manual
   Group      =

   Name       = NlaSvc
   Display    = @%SystemRoot%\System32\nlasvc.dll,-1
   ImagePath  = %SystemRoot%\System32\svchost.exe -k NetworkService
   Type       = Share_Process
   Start      = Auto Start
   Group      =

   Name       = nsi
   Display    = @%SystemRoot%\system32\nsisvc.dll,-200
   ImagePath  = %systemroot%\system32\svchost.exe -k LocalService
   Type       = Share_Process
   Start      = Auto Start
   Group      =

   Name       = NTDS
   Display    =
   ImagePath  =
   Type       =
   Start      =
   Group      =

   Name       = p2pimsvc
   Display    = @%SystemRoot%\system32\pnrpsvc.dll,-8004
   ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
   Type       = Share_Process
   Start      = Manual
   Group      =

   Name       = p2psvc
   Display    = @%SystemRoot%\system32\p2psvc.dll,-8006
   ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
   Type       = Share_Process
   Start      = Manual
   Group      =

   Name       = PcaSvc
   Display    = @%SystemRoot%\system32\pcasvc.dll,-1
   ImagePath  = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
   Type       = Share_Process
   Start      = Auto Start
   Group      =

   Name       = PerfDisk
   Display    =
   ImagePath  =
   Type       =
   Start      =
   Group      =

   Name       = PerfHost
   Display    = @%systemroot%\sysWow64\perfhost.exe,-2
   ImagePath  = %SystemRoot%\SysWow64\perfhost.exe
   Type       = Own_Process
                              Page 116
```

SYSTEM OUTPUT.txt

```
Start      = Manual
Group      =

Name       = PerfNet
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = PerfOS
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = PerfProc
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = pla
Display    = @%systemroot%\system32\pla.dll,-500
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork
Type       = Share_Process
Start      = Manual
Group      =

Name       = PlugPlay
Display    = @%SystemRoot%\system32\umpnpmgr.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type       = Share_Process
Start      = Auto Start
Group      = PlugPlay

Name       = PNRPAutoReg
Display    = @%SystemRoot%\system32\pnrpauto.dll,-8002
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type       = Share_Process
Start      = Manual
Group      =

Name       = PNRPsvc
Display    = @%SystemRoot%\system32\pnrpsvc.dll,-8000
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type       = Share_Process
Start      = Manual
Group      =

Name       = PolicyAgent
Display    = @%SystemRoot%\System32\polstore.dll,-5010
ImagePath  = %SystemRoot%\system32\svchost.exe -k NetworkServiceNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = PortProxy
Display    =
ImagePath  =
Type       =
```

Page 117

SYSTEM OUTPUT.txt

```
Start       =
Group       =

Name        = Power
Display     = @%SystemRoot%\system32\umpo.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type        = Share_Process
Start       = Auto Start
Group       = Plugplay

Name        = ProfSvc
Display     = @%systemroot%\system32\profsvc.dll,-300
ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Auto Start
Group       = profsvc_group

Name        = ProtectedStorage
Display     = @%systemroot%\system32\psbase.dll,-300
ImagePath   = %SystemRoot%\system32\lsass.exe
Type        = Share_Process
Start       = Manual
Group       =

Name        = QWAVE
Display     = @%SystemRoot%\system32\qwave.dll,-1
ImagePath   = %windir%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = QWAVEdrv
Display     = @%SystemRoot%\system32\drivers\qwavedrv.sys,-1
ImagePath   = \SystemRoot\system32\drivers\qwavedrv.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = RasAcd
Display     = Remote Access Auto Connection Driver
ImagePath   = System32\DRIVERS\rasacd.sys
Type        = Kernel driver
Start       = Manual
Group       = Streams Drivers

Name        = RDPDD
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = RDPNP
Display     = @%systemroot%\system32\drprov.dll,-100
ImagePath   =
Type        =
Start       =
Group       =

Name        = RpcLocator
Display     = @%systemroot%\system32\Locator.exe,-2
ImagePath   = %SystemRoot%\system32\locator.exe
Type        = Own_Process
```

Page 118

```
                              SYSTEM OUTPUT.txt
Start        = Manual
Group        =

Name         = RpcSs
Display      = @oleres.dll,-5010
ImagePath    = %SystemRoot%\system32\svchost.exe -k rpcss
Type         = Share_Process
Start        = Auto Start
Group        = COM Infrastructure

Name         = Schedule
Display      = @%SystemRoot%\system32\schedsvc.dll,-100
ImagePath    = %systemroot%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Auto Start
Group        = SchedulerGroup

Name         = SCPolicySvc
Display      = @%SystemRoot%\System32\certprop.dll,-13
ImagePath    = %SystemRoot%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Manual
Group        =

Name         = SDRSVC
Display      = @%SystemRoot%\system32\sdrsvc.dll,-107
ImagePath    = %SystemRoot%\system32\svchost.exe -k SDRSVC
Type         = Own_Process
Start        = Manual
Group        =

Name         = seclogon
Display      = @%SystemRoot%\system32\seclogon.dll,-7001
ImagePath    = %windir%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Manual
Group        =

Name         = SENS
Display      = @%SystemRoot%\system32\Sens.dll,-200
ImagePath    = %SystemRoot%\system32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Auto Start
Group        = ProfSvc_Group

Name         = SharedAccess
Display      = @%SystemRoot%\system32\ipnathlp.dll,-106
ImagePath    = %SystemRoot%\System32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Disabled
Group        =

Name         = ShellHWDetection
Display      = @%SystemRoot%\System32\shsvcs.dll,-12288
ImagePath    = %SystemRoot%\System32\svchost.exe -k netsvcs
Type         = Share_Process
Start        = Auto Start
Group        = ShellSvcGroup

Name         = SNMPTRAP
Display      = @%SystemRoot%\system32\snmptrap.exe,-3
ImagePath    = %SystemRoot%\System32\snmptrap.exe
Type         = Own_Process
                                                    Page 119
```

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       =

Name        = Spooler
Display     = @%systemroot%\system32\spoolsv.exe,-1
ImagePath   = %SystemRoot%\System32\spoolsv.exe
Type        = 0x0
Start       = Auto Start
Group       = SpoolerGroup

Name        = sppsvc
Display     = @%SystemRoot%\system32\sppsvc.exe,-101
ImagePath   = %SystemRoot%\system32\sppsvc.exe
Type        = Own_Process
Start       = Auto Start
Group       =

Name        = sppuinotify
Display     = @%SystemRoot%\system32\sppuinotify.dll,-103
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = SSDPSRV
Display     = @%systemroot%\system32\ssdpsrv.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = SstpSvc
Display     = @%SystemRoot%\system32\sstpsvc.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = stisvc
Display     = @%SystemRoot%\system32\wiaservc.dll,-9
ImagePath   = %SystemRoot%\system32\svchost.exe -k imgsvc
Type        = Own_Process
Start       = Manual
Group       =

Name        = swprv
Display     = @%SystemRoot%\System32\swprv.dll,-103
ImagePath   = %SystemRoot%\System32\svchost.exe -k swprv
Type        = Own_Process
Start       = Manual
Group       =

Name        = SysMain
Display     = @%SystemRoot%\system32\sysmain.dll,-1000
ImagePath   = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = TapiSrv
Display     = @%SystemRoot%\system32\tapisrv.dll,-10100
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
```

Page 120

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       =

Name        = TBS
Display     = @%SystemRoot%\system32\tbssvc.dll,-100
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = TCPIP6TUNNEL
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = TCPIPTUNNEL
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = TDPIPE
Display     = TDPIPE
ImagePath   = system32\drivers\tdpipe.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = TermService
Display     = @%SystemRoot%\System32\termsrv.dll,-268
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =

Name        = Themes
Display     = @%SystemRoot%\System32\themeservice.dll,-8192
ImagePath   = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Auto Start
Group       = ProfSvc_Group

Name        = THREADORDER
Display     = @%systemroot%\system32\mmcss.dll,-102
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = TSDDD
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = UGatherer
Display     =
ImagePath   =
Type        =
```

Page 121

SYSTEM OUTPUT.txt

```
Start      =
Group      =

Name       = UGTHRSVC
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = UI0Detect
Display    = @%SystemRoot%\system32\ui0detect.exe,-101
ImagePath  = %SystemRoot%\system32\UI0Detect.exe
Type       = 0x0
Start      = Manual
Group      =

Name       = upnphost
Display    = @%systemroot%\system32\upnphost.dll,-213
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type       = Share_Process
Start      = Manual
Group      =

Name       = UxSms
Display    = @%SystemRoot%\system32\dwm.exe,-2000
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type       = Share_Process
Start      = Auto Start
Group      = UIGroup

Name       = VaultSvc
Display    = @%SystemRoot%\system32\vaultsvc.dll,-1003
ImagePath  = %SystemRoot%\system32\lsass.exe
Type       = Share_Process
Start      = Manual
Group      =

Name       = vds
Display    = @%SystemRoot%\system32\vds.exe,-100
ImagePath  = %SystemRoot%\System32\vds.exe
Type       = Own_Process
Start      = Manual
Group      =

Name       = VSS
Display    = @%systemroot%\system32\vssvc.exe,-102
ImagePath  = %systemroot%\system32\vssvc.exe
Type       = Own_Process
Start      = Manual
Group      =

Name       = W3SVC
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = wbengine
Display    = @%systemroot%\system32\wbengine.exe,-104
ImagePath  = "%systemroot%\system32\wbengine.exe"
Type       = Own_Process
```

Page 122

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       =

Name        = wcncsvc
Display     = @%SystemRoot%\system32\wcncsvc.dll,-3
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = WcsPlugInService
Display     = @%SystemRoot%\system32\WcsPlugInService.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k wcssvc
Type        = Share_Process
Start       = Manual
Group       =

Name        = Wecsvc
Display     = @%SystemRoot%\system32\wecsvc.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =

Name        = wercplsupport
Display     = @%SystemRoot%\System32\wercplsupport.dll,-101
ImagePath   = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = WerSvc
Display     = @%SystemRoot%\System32\wersvc.dll,-100
ImagePath   = %SystemRoot%\System32\svchost.exe -k WerSvcGroup
Type        = Share_Process
Start       = Manual
Group       =

Name        = WIMMount
Display     = WIMMount
ImagePath   = system32\drivers\wimmount.sys
Type        = File system driver
Start       = Manual
Group       = FSFilter Infrastructure

Name        = WinHttpAutoProxySvc
Display     = @%SystemRoot%\system32\winhttp.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = WinRM
Display     = @%Systemroot%\system32\wsmsvc.dll,-101
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =

Name        = WinSock2
Display     =
ImagePath   =
Type        =
```

Page 123

SYSTEM OUTPUT.txt

```
Start       =
Group       =

Name        = WMPNetworkSvc
Display     = @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101
ImagePath   = "%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe"
Type        = Own_Process
Start       = Manual
Group       =

Name        = WPDBusEnum
Display     = @%SystemRoot%\system32\wpdbusenum.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = ws2ifsl
Display     = @%systemroot%\System32\drivers\ws2ifsl.sys,-1000
ImagePath   = \SystemRoot\system32\drivers\ws2ifsl.sys
Type        = Kernel driver
Start       = Disabled
Group       = PNP_TDI

Name        = wscsvc
Display     = @%SystemRoot%\System32\wscsvc.dll,-200
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = WSearchIdxPi
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = WwanSvc
Display     = @%SystemRoot%\System32\wwansvc.dll,-257
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork
Type        = Share_Process
Start       = Manual
Group       = TDI

Name        = xmlprov
Display     =
ImagePath   =
Type        =
Start       =
Group       =

-----------------------------------
shares v.20140730
(System) Get list of shares from System hive file

 subkey not found.
-----------------------------------
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
```

Page 124

SYSTEM OUTPUT.txt
LastWrite Time Wed Apr 20 15:40:04 2016 (UTC)
  ShutdownTime = Wed Apr 20 15:40:04 2016 (UTC)
----------------------------------------
shutdowncount v.20080709
(System) Retrieves ShutDownCount value

ControlSet001\Control\Watchdog\Display not found.
----------------------------------------
stillimage v.20100222
(System) Get info on StillImage devices


StillImage Logging Level
  STICLI Logging Level = 0x4
  STIMON Logging Level = 0x4
----------------------------------------
svc v.20131010
(System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName
Thu Apr 28 15:00:49 2016 Z,mferkdet,McAfee Inc.
mferkdet,system32\drivers\mferkdet.sys,Kernel driver,Manual,,McAfee NDIS Light
Filter
Thu Apr 28 15:00:38 2016 Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,,Allows scheduling of
McAfee scanning and updating activities.
Thu Apr 28 15:00:36 2016 Z,mfeapfk,McAfee Inc.
mfeapfk,system32\drivers\mfeapfk.sys,Kernel driver,Manual,,Allows scheduling of
McAfee scanning and updating activities.
Wed Apr 20 15:58:48 2016
Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\se
rvicing\TrustedInstaller.exe,Own_Process,Manual,localSystem,@%SystemRoot%\servicing\
TrustedInstaller.exe,-101
Wed Apr 20 15:42:05 2016 Z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,Kernel driver,Boot Start,,Provides firewall
services to McAfee products
Wed Apr 20 15:42:04 2016 Z,DisplayLinkService,DisplayLinkManager,"C:\Program
Files\DisplayLink Core Software\DisplayLinkManager.exe",Own_Process,Auto
Start,LocalSystem,Manages DisplayLink Graphics Adapters according to Windows display
properties
Wed Apr 20 15:41:02 2016
Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asyncmac.sys,Ke
rnel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32000
Wed Apr 20 15:40:59 2016
Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,,
Wed Apr 20 15:40:59 2016 Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,Kernel driver,Manual,,Allows scheduling of
McAfee scanning and updating activities.
Wed Apr 20 15:40:59 2016 Z,mfeavfk01,McAfee Inc.,,Kernel driver,Manual,,Allows
scheduling of McAfee scanning and updating activities.
Wed Apr 20 15:40:59 2016 Z,mfemms,McAfee Service Controller,"C:\Program Files\Common
Files\McAfee\SystemCore\\mfemms.exe",Own_Process,Auto Start,LocalSystem,Manages
McAfee Services
Wed Apr 20 15:40:59 2016
Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,,
Wed Apr 20 15:40:59 2016
Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,,
Wed Apr 20 15:40:52 2016 Z,cvusbdrv,Dell
ControlVault,System32\Drivers\cvusbdrv.sys,Kernel
driver,Manual,,@%systemroot%\system32\cscsvc.dll,-201
Wed Apr 20 15:40:52 2016 Z,kbdhid,Keyboard HID
Driver,system32\DRIVERS\kbdhid.sys,Kernel
Page 125

SYSTEM OUTPUT.txt
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Wed Apr 20 15:40:52 2016 Z,mouhid,Mouse HID
Driver,system32\DRIVERS\mouhid.sys,Kernel
driver,Manual,,@%systemroot%\system32\mmcss.dll,-101
Wed Apr 20 15:40:52 2016
Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfilter
.sys,Kernel driver,Manual,,@%SystemRoot%\System32\drivers\scfilter.sys,-12
Wed Apr 20 15:40:52 2016 Z,WinUsb,WinUSB Driver,system32\DRIVERS\WinUSB.sys,Kernel
driver,Manual,,@%systemroot%\system32\wsmsvc.dll,-102
Wed Apr 20 15:40:51 2016 Z,HidUsb,Microsoft HID Class
Driver,system32\DRIVERS\hidusb.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\hidserv.dll,-102
Wed Apr 20 15:40:51 2016 Z,monitor,Microsoft Monitor Class Function Driver
Service,system32\DRIVERS\monitor.sys,Kernel
driver,Manual,,@%systemroot%\system32\mmcss.dll,-101
Wed Apr 20 15:40:51 2016 Z,usbccgp,Microsoft USB Generic Parent
Driver,system32\DRIVERS\usbccgp.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Apr 20 15:40:51 2016 Z,usbvideo,USB Video Device
(WDM),System32\Drivers\usbvideo.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Apr 20 15:40:50 2016 Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,,Provides firewall
services to McAfee products
Wed Apr 20 15:40:49 2016 Z,IntcAzAudAddService,Service for Realtek HD Audio
(WDM),system32\drivers\RTDVHD64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Wed Apr 20 15:40:49 2016 Z,iusb3hub,Intel(R) USB 3.0 Hub
Driver,system32\DRIVERS\iusb3hub.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Wed Apr 20 15:40:49 2016 Z,ST_Accel,STMicroelectronics Accelerometer
Service,system32\DRIVERS\ST_Accel.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\StorSvc.dll,-101
Wed Apr 20 15:40:48 2016 Z,IntcDAud,Intel(R) Display
Audio,system32\DRIVERS\IntcDAud.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Wed Apr 20 15:40:48 2016 Z,ksthunk,Kernel Streaming
Thunks,\SystemRoot\system32\drivers\ksthunk.sys,Kernel
driver,Manual,,@keyiso.dll,-101
Wed Apr 20 15:40:48 2016 Z,Parport,Parallel port
driver,system32\DRIVERS\parport.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\p2psvc.dll,-8007
Wed Apr 20 15:40:48 2016 Z,usbhub,Microsoft USB Standard Hub
Driver,system32\DRIVERS\usbhub.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Apr 20 15:40:47 2016 Z,mssmbios,Microsoft System Management BIOS
Driver,system32\DRIVERS\mssmbios.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\msimsg.dll,-32
Wed Apr 20 15:40:46 2016 Z,nvlddmkm,,system32\DRIVERS\nvlddmkm.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Wed Apr 20 15:40:46 2016 Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel
driver,Boot Start,,ReadyBoost
Wed Apr 20 15:40:45 2016 Z,ACPI,Microsoft ACPI
Driver,system32\drivers\ACPI.sys,Kernel driver,Boot Start,,Provide access to the
shared store. If this service is stopped or disabled, ActivIdentity products will
not function properly.
Wed Apr 20 15:40:45 2016 Z,acsock,acsock,system32\DRIVERS\acsock64.sys,Kernel
driver,Manual,,Cisco AnyConnect Kernel Driver Framework Socket Layer Interceptor
Wed Apr 20 15:40:45 2016
Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\afd.
sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\afd.sys,-1000
Wed Apr 20 15:40:45 2016 Z,ApfiltrService,Alps Touch Pad Filter Driver for Windows
x64,system32\DRIVERS\Apfiltr.sys,Kernel
Page 126

```
SYSTEM OUTPUT.txt
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Wed Apr 20 15:40:45 2016 Z,Beep,Beep,,Kernel driver,System
Start,,@%SystemRoot%\system32\bdesvc.dll,-101
Wed Apr 20 15:40:45 2016 Z,blbdrive,,system32\DRIVERS\blbdrive.sys,Kernel
driver,System Start,,@%SystemRoot%\system32\qmgr.dll,-1001
Wed Apr 20 15:40:45 2016
Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,File
system driver,Manual,,@%systemroot%\system32\browser.dll,-103
Wed Apr 20 15:40:45 2016 Z,CipcCdp,Cisco IP Communicator driver for
CDP,system32\DRIVERS\CipcCdp.sys,Kernel driver,Auto Start,,Cisco IP Communicator
driver for CDP
Wed Apr 20 15:40:45 2016
Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,System32\CLFS.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\clfs.sys,-101
Wed Apr 20 15:40:45 2016 Z,CmBatt,Microsoft ACPI Control Method Battery
Driver,system32\DRIVERS\CmBatt.sys,Kernel driver,Manual,,Microsoft .NET Framework
NGEN
Wed Apr 20 15:40:45 2016 Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot
Start,,Provides the ability to remote control the system to authorized users
Wed Apr 20 15:40:45 2016 Z,Compbatt,Microsoft Composite Battery
Driver,system32\DRIVERS\compbatt.sys,Kernel driver,Boot Start,,Provides the ability
to remote control the system to authorized users
Wed Apr 20 15:40:45 2016 Z,CompositeBus,Composite Bus Enumerator
Driver,system32\DRIVERS\CompositeBus.sys,Kernel driver,Manual,,Provides the ability
to remote control the system to authorized users
Wed Apr 20 15:40:45 2016
Z,CSC,@%systemroot%\system32\cscsvc.dll;-202,system32\drivers\csc.sys,Kernel
driver,System Start,,@%systemroot%\system32\cscsvc.dll,-203
Wed Apr 20 15:40:45 2016 Z,ctxusbm,Citrix USB Monitor
Driver,system32\DRIVERS\ctxusbm.sys,Kernel driver,System
Start,,@%systemroot%\system32\cscsvc.dll,-201
Wed Apr 20 15:40:45 2016 Z,CVirtA,Cisco Systems VPN Adapter for 64-bit
Windows,system32\DRIVERS\CVirtA64.sys,Kernel
driver,Manual,,@%systemroot%\system32\cscsvc.dll,-201
Wed Apr 20 15:40:45 2016 Z,CVPNDRVA,Cisco Systems Inc. IPSec
Driver,\??\C:\WINDOWS\system32\Drivers\CVPNDRVA.sys,Kernel
driver,Manual,,@%systemroot%\system32\cscsvc.dll,-201
Wed Apr 20 15:40:45 2016
Z,DfsC,@%systemroot%\system32\drivers\dfsc.sys;-101,System32\Drivers\dfsc.sys,File
system driver,System Start,,@%systemroot%\system32\drivers\dfsc.sys,-102
Wed Apr 20 15:40:45 2016
Z,discache,@%systemroot%\system32\drivers\discache.sys;-102,System32\drivers\discach
e.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\discache.sys,-101
Wed Apr 20 15:40:45 2016 Z,Disk,Disk Driver,system32\drivers\disk.sys,Kernel
driver,Boot Start,,@%systemroot%\system32\drivers\discache.sys,-101
Wed Apr 20 15:40:45 2016 Z,DNE,Deterministic Network Enhancer
Miniport,system32\DRIVERS\dne64x.sys,Kernel driver,Manual,,Manages DisplayLink
Graphics Adapters according to Windows display properties
Wed Apr 20 15:40:45 2016 Z,dptf_acpi,,system32\DRIVERS\dptf_acpi.sys,Kernel
driver,Manual,,@%systemroot%\system32\dps.dll,-501
Wed Apr 20 15:40:45 2016 Z,dptf_cpu,,system32\DRIVERS\dptf_cpu.sys,Kernel
driver,Manual,,@%systemroot%\system32\dps.dll,-501
Wed Apr 20 15:40:45 2016 Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,,Controls
the underlying video driver stacks to provide fully-featured display capabilities.
Wed Apr 20 15:40:45 2016 Z,e1dexpress,Intel(R) PRO/1000 PCI Express Network
Connection Driver D,system32\DRIVERS\e1d62x64.sys,Kernel driver,Manual,,Controls the
underlying video driver stacks to provide fully-featured display capabilities.
Wed Apr 20 15:40:45 2016
Z,enstart64_,enstart64_,\??\C:\WINDOWS\system32\enstart64_.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\efsvc.dll,-101
Wed Apr 20 15:40:45 2016 Z,esif_lf,,system32\DRIVERS\esif_lf.sys,Kernel
driver,Manual,,Host-based intrusion prevention component that blocks exploits and
Page 127
```

SYSTEM OUTPUT.txt
hacks in real-time, including malicious buffer overflow code execution and privilege
escalations. If this service is disabled or stopped, the system is no longer
protected against intrusions.
Wed Apr 20 15:40:45 2016
Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,system32\drivers\fileinf
o.sys,File system driver,Boot
Start,,@%SystemRoot%\system32\drivers\fileinfo.sys,-101
Wed Apr 20 15:40:45 2016
Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmgr.sy
s,File system driver,Boot Start,,@%SystemRoot%\system32\drivers\fltmgr.sys,-10000
Wed Apr 20 15:40:45 2016 Z,Fs_Rec,,,8,Boot
Start,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000
Wed Apr 20 15:40:45 2016
Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.sys,
Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\fvevol.sys,-100
Wed Apr 20 15:40:45 2016 Z,HDAudBus,Microsoft UAA Bus Driver for High Definition
Audio,system32\DRIVERS\HDAudBus.sys,Kernel driver,Manual,,Keeps your Google software
up to date. If this service is disabled or stopped, your Google software will not be
kept up to date, meaning security vulnerabilities that may arise cannot be fixed and
features may not work. This service uninstalls itself when there is no Google
software using it.
Wed Apr 20 15:40:45 2016
Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\http.sys,-2
Wed Apr 20 15:40:45 2016
Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwpolic
y.sys,Kernel driver,Boot Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Wed Apr 20 15:40:45 2016 Z,i8042prt,i8042 Keyboard and PS/2 Mouse Port
Driver,system32\DRIVERS\i8042prt.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Wed Apr 20 15:40:45 2016 Z,iaStorA,,system32\drivers\iaStorA.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Wed Apr 20 15:40:45 2016 Z,iaStorF,,system32\drivers\iaStorF.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Wed Apr 20 15:40:45 2016 Z,igfx,,system32\DRIVERS\igdkmd64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001
Wed Apr 20 15:40:45 2016 Z,intelppm,Intel Processor
Driver,system32\DRIVERS\intelppm.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Wed Apr 20 15:40:45 2016 Z,iusb3xhc,Intel(R) USB 3.0 eXtensible Host Controller
Driver,system32\DRIVERS\iusb3xhc.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Wed Apr 20 15:40:45 2016 Z,kbdclass,Keyboard Class
Driver,system32\DRIVERS\kbdclass.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Wed Apr 20 15:40:45 2016 Z,KSecDD,,System32\Drivers\ksecdd.sys,Kernel driver,Boot
Start,,@keyiso.dll,-101
Wed Apr 20 15:40:45 2016 Z,KSecPkg,,System32\Drivers\ksecpkg.sys,Kernel driver,Boot
Start,,@keyiso.dll,-101
Wed Apr 20 15:40:45 2016 Z,lltdio,Link-Layer Topology Discovery Mapper I/O
Driver,system32\DRIVERS\lltdio.sys,Kernel driver,Auto
Start,,@%systemroot%\system32\wkssvc.dll,-101
Wed Apr 20 15:40:45 2016
Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drivers\l
uafv.sys,File system driver,Auto
Start,,@%systemroot%\system32\drivers\luafv.sys,-101
Wed Apr 20 15:40:45 2016 Z,MEIx64,Intel(R) Management Engine Interface
,system32\DRIVERS\TeeDriverx64.sys,Kernel driver,Manual,,Allows scheduling of McAfee
scanning and updating activities.
Wed Apr 20 15:40:45 2016 Z,mfenlfk,McAfee NDIS Light
Filter,system32\DRIVERS\mfenlfk.sys,Kernel driver,System Start,,McAfee NDIS Light
Filter
Wed Apr 20 15:40:45 2016 Z,mfewfpk,McAfee Inc.
Page 128

SYSTEM OUTPUT.txt
mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,,Provides validation
trust protection services
Wed Apr 20 15:40:45 2016 Z,mouclass,Mouse Class
Driver,system32\DRIVERS\mouclass.sys,Kernel
driver,Manual,,@%systemroot%\system32\mmcss.dll,-101
Wed Apr 20 15:40:45 2016
Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mountmg
r.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\mountmgr.sys,-101
Wed Apr 20 15:40:45 2016
Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,System32\drivers\mpsdrv.sys,K
ernel driver,Manual,,@%SystemRoot%\system32\FirewallAPI.dll,-23093
Wed Apr 20 15:40:45 2016
Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mrxdav
.sys,File system driver,Manual,,@%systemroot%\system32\webclnt.dll,-105
Wed Apr 20 15:40:45 2016
Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,File
system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1003
Wed Apr 20 15:40:45 2016
Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys,Fil
e system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1005
Wed Apr 20 15:40:45 2016
Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys,Fil
e system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1007
Wed Apr 20 15:40:45 2016 Z,Msfs,,,File system driver,System Start,,@comres.dll,-2798
Wed Apr 20 15:40:45 2016 Z,msisadrv,,system32\drivers\msisadrv.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\mshidkmdf.sys,-101
Wed Apr 20 15:40:45 2016
Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,File
system driver,Boot Start,,@%systemroot%\system32\drivers\mup.sys,-102
Wed Apr 20 15:40:45 2016 Z,NativeWifiP,NativeWiFi
Filter,system32\DRIVERS\nwifi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\qagentrt.dll,-7
Wed Apr 20 15:40:45 2016
Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\ndis.sys,-201
Wed Apr 20 15:40:45 2016
Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sys,Ke
rnel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001
Wed Apr 20 15:40:45 2016 Z,Ndisuio,NDIS Usermode I/O
Protocol,system32\DRIVERS\ndisuio.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001
Wed Apr 20 15:40:45 2016
Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,Kern
el driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002
Wed Apr 20 15:40:45 2016 Z,NDProxy,NDIS Proxy,,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002
Wed Apr 20 15:40:45 2016 Z,NetBIOS,NetBIOS
Interface,system32\DRIVERS\netbios.sys,File system driver,System Start,,NetBIOS
Interface
Wed Apr 20 15:40:45 2016
Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,Kerne
l driver,System Start,,@%SystemRoot%\system32\drivers\netbt.sys,-1
Wed Apr 20 15:40:45 2016 Z,NETwNs64,___ Intel(R) Wireless Adapter Driver for Windows
7 - 64 Bit,system32\DRIVERS\Netwsw02.sys,Kernel
driver,Manual,,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstall
RC.dll,-8200
Wed Apr 20 15:40:45 2016 Z,Npfs,,,File system driver,System
Start,,@%SystemRoot%\System32\nlasvc.dll,-2
Wed Apr 20 15:40:45 2016.
Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsiproxy.
sys,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Wed Apr 20 15:40:45 2016 Z,Ntfs,,,File system
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Page 129

SYSTEM OUTPUT.txt

Wed Apr 20 15:40:45 2016 Z,Null,,,Kernel driver,System
Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Wed Apr 20 15:40:45 2016 Z,nvpciflt,,system32\DRIVERS\nvpciflt.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Wed Apr 20 15:40:45 2016 Z,O2FJ2RDR,,system32\DRIVERS\O2FJ2w7x64.sys,Kernel
driver,Manual,,Provides system and desktop level support to the NVIDIA display
driver
Wed Apr 20 15:40:45 2016
Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partmgr.s
ys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\partmgr.sys,-101
Wed Apr 20 15:40:45 2016 Z,pci,PCI Bus Driver,system32\drivers\pci.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Wed Apr 20 15:40:45 2016 Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Wed Apr 20 15:40:45 2016 Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel
driver,Auto Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Wed Apr 20 15:40:45 2016
Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp.sys
,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32006
Wed Apr 20 15:40:45 2016 Z,prepdrvr,SMS Process Event
Driver,system32\DRIVERS\prepdrv.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32006
Wed Apr 20 15:40:45 2016 Z,prot_2k,,,Kernel driver,Boot
Start,,@%systemroot%\system32\psbase.dll,-301
Wed Apr 20 15:40:45 2016
Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sys,Ke
rnel driver,System Start,,@%SystemRoot%\System32\drivers\pacer.sys,-101
Wed Apr 20 15:40:45 2016 Z,RasAgileVpn,WAN Miniport
(IKEv2),system32\DRIVERS\AgileVpn.sys,Kernel driver,Manual,,WAN Miniport (IKEv2)
Wed Apr 20 15:40:45 2016
Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,Kern
el driver,Manual,,@%systemroot%\system32\rascfg.dll,-32005
Wed Apr 20 15:40:45 2016
Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\raspppoe.sys,Ke
rnel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32007
Wed Apr 20 15:40:45 2016
Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,Kerne
l driver,Manual,,@%systemroot%\system32\sstpsvc.dll,-202
Wed Apr 20 15:40:45 2016
Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File
system driver,System Start,,@%systemroot%\system32\wkssvc.dll,-1001
Wed Apr 20 15:40:45 2016 Z,rdpbus,Remote Desktop Device Redirector Bus
Driver,system32\DRIVERS\rdpbus.sys,Kernel
driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1001
Wed Apr 20 15:40:45 2016
Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,System32\DRIVERS\RDPCDD.sys,
Kernel driver,System Start,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101
Wed Apr 20 15:40:45 2016 Z,RDPDR,Terminal Server Device Redirector
Driver,System32\drivers\rdpdr.sys,Kernel
driver,Manual,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101
Wed Apr 20 15:40:45 2016
Z,RDPENCDD,@%systemroot%\system32\drivers\RDPENCDD.sys;-101,system32\drivers\rdpencd
d.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\RDPENCDD.sys,-100
Wed Apr 20 15:40:45 2016
Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdprefm
p.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100
Wed Apr 20 15:40:45 2016 Z,RDPWD,RDP Winstation Driver,,Kernel
driver,Manual,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100
Wed Apr 20 15:40:45 2016 Z,rspndr,Link-Layer Topology Discovery
Responder,system32\DRIVERS\rspndr.sys,Kernel driver,Auto Start,,@oleres.dll,-5011
Wed Apr 20 15:40:45 2016 Z,Serenum,Serenum Filter
Driver,system32\DRIVERS\serenum.sys,Kernel

Page 130

SYSTEM OUTPUT.txt

driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Wed Apr 20 15:40:45 2016 Z,Serial,Serial port
driver,system32\DRIVERS\serial.sys,Kernel driver,System
Start,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Wed Apr 20 15:40:45 2016 Z,spldr,Security Processor Loader Driver,,Kernel
driver,Boot Start,,@%SystemRoot%\system32\snmptrap.exe,-4
Wed Apr 20 15:40:45 2016
Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,File system
driver,Manual,,@%systemroot%\system32\srvsvc.dll,-103
Wed Apr 20 15:40:45 2016
Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,File system
driver,Manual,,@%systemroot%\system32\srvsvc.dll,-105
Wed Apr 20 15:40:45 2016 Z,srvnet,,System32\DRIVERS\srvnet.sys,File system
driver,Manual,,@%systemroot%\system32\srvsvc.dll,-105
Wed Apr 20 15:40:45 2016 Z,stdcfltn,Disk Class Filter Driver for
Accelerometer,system32\DRIVERS\stdcfltn.sys,Kernel driver,Boot
start,,@%SystemRoot%\system32\sstpsvc.dll,-201
Wed Apr 20 15:40:45 2016 Z,swenum,Software Bus
Driver,system32\DRIVERS\swenum.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\StorSvc.dll,-101
Wed Apr 20 15:40:45 2016
Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50003
Wed Apr 20 15:40:45 2016 Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,,Provides
compatibility for legacy applications which interact with TCP/IP through the
registry. If this service is stopped, certain applications may have impaired
functionality.
Wed Apr 20 15:40:45 2016 Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,Kernel
driver,Manual,,Provides compatibility for legacy applications which interact with
TCP/IP through the registry. If this service is stopped, certain applications may
have impaired functionality.
Wed Apr 20 15:40:45 2016
Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,System32\DRIVERS\tdx.sys,Kernel
driver,System Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50004
Wed Apr 20 15:40:45 2016 Z,TermDD,Terminal Device
Driver,system32\DRIVERS\termdd.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50004
Wed Apr 20 15:40:45 2016
Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,System32\DRIVERS\tssecsr
v.sys,Kernel driver,Manual,,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys,-102
Wed Apr 20 15:40:45 2016 Z,tunnel,Microsoft Tunnel Miniport Adapter
Miniport Driver,system32\DRIVERS\tunnel.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Apr 20 15:40:45 2016 Z,vdrvroot,Microsoft Virtual Drive Enumerator
Driver,system32\drivers\vdrvroot.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\vaultsvc.dll,-1004
Wed Apr 20 15:40:45 2016 Z,VgaSave,,\SystemRoot\System32\drivers\vga.sys,Kernel
driver,System Start,,@%SystemRoot%\system32\vds.exe,-112
Wed Apr 20 15:40:45 2016 Z,volmgr,Volume Manager
Driver,system32\drivers\volmgr.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\vds.exe,-112
Wed Apr 20 15:40:45 2016
Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmgrx.s
ys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101
Wed Apr 20 15:40:45 2016 Z,volsnap,Storage
volumes,system32\drivers\volsnap.sys,Kernel driver,Boot
Page 131

SYSTEM OUTPUT.txt
Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101
Wed Apr 20 15:40:45 2016 Z,vpnva,Cisco AnyConnect Secure Mobility Client Virtual
Miniport Adapter for Windows x64,system32\DRIVERS\vpnva64-6.sys,Kernel
driver,Manual,,Cisco AnyConnect Secure Mobility Agent for Windows
Wed Apr 20 15:40:45 2016 Z,vwifibus,Virtual WiFi Bus
Driver,system32\DRIVERS\vwifibus.sys,Kernel driver,Manual,,Virtual WiFi Bus Driver
Wed Apr 20 15:40:45 2016 Z,vwififlt,Virtual WiFi Filter
Driver,system32\DRIVERS\vwififlt.sys,Kernel driver,System Start,,Virtual WiFi Filter
Driver
Wed Apr 20 15:40:45 2016
Z,Wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,system32\DRIVERS\wanarp.sys,Kern
el driver,System Start,,@%systemroot%\system32\rascfg.dll,-32012
Wed Apr 20 15:40:45 2016
Z,wdf01000,@%SystemRoot%\system32\drivers\wdf01000.sys;-1000,system32\drivers\wdf010
00.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\WcsPlugInService.dll,-201
Wed Apr 20 15:40:45 2016 Z,WfpLwf,WFP Lightweight
Filter,system32\DRIVERS\wfplwf.sys,Kernel driver,System Start,,WFP Lightweight
Filter
Wed Apr 20 15:40:45 2016 Z,WmiAcpi,Microsoft Windows Management Interface for
ACPI,system32\DRIVERS\wmiacpi.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wlansvc.dll,-258
Wed Apr 20 15:40:45 2016
Z,WudfPf,@%SystemRoot%\system32\drivers\wudfpf.sys;-1000,system32\drivers\WudfPf.sys
,Kernel driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106
Wed Apr 20 15:40:45 2016 Z,WUDFRd,Windows Driver Foundation - User-mode Driver
Framework Reflector,system32\DRIVERS\WUDFRd.sys,Kernel
driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106
Wed Apr 20 15:39:52 2016 Z,drmkaud,Microsoft Trusted Audio
Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel
driver,Manual,,@%systemroot%\system32\dps.dll,-501
Wed Apr 20 13:19:57 2016 Z,macmnsvc,McAfee Agent Common Services,"C:\Program Files
(x86)\McAfee\Common Framework\macmnsvc.exe" /ServiceStart,Own_Process,Auto Start,NT
AUTHORITY\LocalService,McAfee Agent Common Services
Wed Apr 20 13:19:57 2016 Z,masvc,McAfee Agent Service,"C:\Program Files
(x86)\McAfee\Common Framework\masvc.exe" /ServiceStart,Own_Process,Auto
Start,LocalSystem,McAfee Agent Service
Wed Apr 20 13:19:57 2016 Z,McAfeeFramework,McAfee Agent Backwards Compatibility
Service,"C:\Program Files (x86)\McAfee\Common
Framework\x86\macompatsvc.exe",Own_Process,Manual,LocalSystem,McAfee Agent Backwards
Compatibility Service
Wed Apr 20 13:19:43 2016 Z,mfefire,McAfee Firewall Core Service,"C:\Program
Files\Common
Files\McAfee\SystemCore\\mfefire.exe",Own_Process,Manual,LocalSystem,Provides
firewall services to McAfee products
Wed Apr 20 13:19:40 2016 Z,McShield,McAfee McShield,"C:\Program Files\Common
Files\McAfee\SystemCore\\mcshield.exe",Own_Process,Auto Start,LocalSystem,McAfee
OnAccess Scanner
Wed Apr 20 13:19:38 2016 Z,mfevtp,McAfee Validation Trust Protection
Service,"C:\WINDOWS\system32\mfevtps.exe",Own_Process,Auto
Start,LocalSystem,Provides validation trust protection services
Wed Apr 20 13:19:10 2016 Z,enterceptAgent,McAfee Host Intrusion Prevention
Service,"C:\Program Files\McAfee\Host Intrusion
Prevention\FireSvc.exe",Own_Process,Auto Start,LocalSystem,Host-based intrusion
prevention component that blocks exploits and hacks in real-time, including
malicious buffer overflow code execution and privilege escalations. If this service
is disabled or stopped, the system is no longer protected against intrusions.
Tue Apr 19 20:40:52 2016 Z,MozillaMaintenance,Mozilla Maintenance
Service,"C:\Program Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe",Own_Process,Manual,LocalSystem,The Mozilla
Maintenance Service ensures that you have the latest and most secure version of
Mozilla Firefox on your computer. Keeping Firefox up to date is very important for
your online security, and Mozilla strongly recommends that you keep this service
enabled.
Page 132

SYSTEM OUTPUT.txt

Tue Apr 19 20:40:07 2016 Z,gupdate,Google Update Service (gupdate),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc,Own_Process,Auto Start,LocalSystem,keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Tue Apr 19 20:40:07 2016 Z,gupdatem,Google Update Service (gupdatem),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,Own_Process,Manual,LocalSystem,keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Tue Apr 19 20:03:56 2016 Z,MSDTC,@comres.dll,-2797,"%SystemRoot%\System32\msdtc.exe,Own_Process,Manual,NT AUTHORITY\NetworkService,@comres.dll,-2798"

Tue Apr 19 20:00:35 2016 Z,CmRcService,Configuration Manager Remote Control,"C:\WINDOWS\CCM\RemCtrl\CmRcService.exe,Own_Process,Auto Start,LocalSystem,Provides the ability to remote control the system to authorized users

Tue Apr 19 20:00:19 2016 Z,ccmframework,,,,,,Provides change and configuration services for computer management systems.

Tue Apr 19 19:48:22 2016 Z,USBSTOR,USB Mass Storage Driver,system32\DRIVERS\USBSTOR.SYS,Kernel driver,Manual,,"@%systemroot%\system32\upnphost.dll,-214

Tue Apr 19 19:47:44 2016 Z,EapHost,@%SystemRoot%\System32\eapsvc.dll,-1,"%SystemRoot%\System32\svchost.exe -k netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\eapsvc.dll,-2

Mon Apr 18 16:26:07 2016 Z,MSKSSRV,Microsoft Streaming Service Proxy,system32\drivers\MSKSSRV.sys,kernel driver,Manual,,"@%SystemRoot%\System32\msimsg.dll,-32

Mon Apr 18 16:17:34 2016 Z,ipsec,,,,,"@%SystemRoot%\system32\iphlpsvc.dll,-501

Mon Apr 18 16:17:34 2016 Z,RasMan,Parameters,,"%SystemRoot%\System32\rasmans.dll,,,,

Mon Apr 18 16:17:30 2016 Z,Browser,Computer Browser,%SystemRoot%\System32\svchost.exe -k netsvcs,Share_Process,Disabled,LocalSystem,@%systemroot%\system32\browser.dll,-101

Mon Apr 18 16:17:30 2016 Z,HomeGroupListener,Homegroup Listener,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Disabled,LocalSystem,@%SystemRoot%\System32\listsvc.dll,-101

Mon Apr 18 16:17:30 2016 Z,HomeGroupProvider,Homegroup Provider,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,Share_Process,Disabled,NT AUTHORITY\LocalService,@%SystemRoot%\System32\provsvc.dll,-101

Mon Apr 18 16:17:30 2016 Z,WPCSvc,Parental Control,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,Share_Process,Disabled,NT AUTHORITY\LocalService,@%SystemRoot%\System32\wpcsvc.dll,-101

Mon Apr 18 16:03:47 2016 Z,HipShieldk,McAfee Inc.,HipShieldk,system32\drivers\HipShieldk.sys,Kernel driver,Manual,,Host-based intrusion prevention component that implements the McAfee HA Ipc interface

Mon Apr 18 16:02:36 2016 Z,HIpMgmt,McAfee Host Intrusion Prevention Ipc Service,"C:\Program Files (x86)\McAfee\Host Intrusion Prevention\HipMgmt.exe","Own_Process,Auto Start,LocalSystem,Host-based Intrusion prevention component that implements the McAfee HA Ipc interface

Mon Apr 18 16:02:15 2016 Z,FireNTcp,McAfee Inc. FireNTcp,system32\drivers\FireNTcp.sys,kernel driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000

Mon Apr 18 15:58:37 2016 Z,mcTaskManager,McAfee Task Manager","C:\Program Files (x86)\McAfee\VirusScan Enterprise\VsTskMgr.exe","Own_Process,Auto Start,LocalSystem,Allows scheduling of McAfee scanning and updating activities.

Mon Apr 18 15:58:26 2016 Z,SMMP,,,,,,Configmgr client agent for task sequence execution

Page 133

SYSTEM OUTPUT.txt

Mon Apr 18 15:57:48 2016 Z,PCP,,,,,,@%SystemRoot%\system32\pcasvc.dll,-2
Mon Apr 18 15:57:46 2016
Z,eventlog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\wevtsvc.dll,-201
Mon Apr 18 15:57:46 2016
Z,Pointsec,Pointsec,C:\WINDOWS\SysWOW64\Prot_srv.exe,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\pnrpsvc.dll,-8001
Mon Apr 18 15:57:46 2016 Z,Pointsec_Start,Pointsec Service
Start,C:\WINDOWS\SysWOW64\PstartSr.exe,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\pnrpsvc.dll,-8001
Mon Apr 18 15:57:14 2016 Z,CVPND,Cisco Systems; Inc. VPN Service,"C:\Program Files
(x86)\Cisco Systems\VPN Client\cvpnd.exe",Own_Process,Auto
Start,LocalSystem,@%systemroot%\system32\cscsvc.dll,-201
Mon Apr 18 15:57:04 2016
Z,{2A088A0C-A99B-4B11-81C8-178260EEB892},,,,,,@%SystemRoot%\System32\wwansvc.dll,-25
8
Mon Apr 18 15:56:59 2016
Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,,
Mon Apr 18 15:56:53 2016
Z,{915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3},,,,,,@%SystemRoot%\System32\wwansvc.dll,-25
8
Mon Apr 18 15:56:52 2016 Z,vpnagent,Cisco AnyConnect Secure Mobility
Agent,"C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\vpnagent.exe",Own_Process,Auto Start,LocalSystem,Cisco AnyConnect Secure
Mobility Agent for Windows
Mon Apr 18 15:54:46 2016 Z,atashost,WebEx Service Host for Support
Center,"C:\WINDOWS\SysWOW64\atashost.exe",Own_Process,Auto Start,LocalSystem,WebEx
Support Center.
Mon Apr 18 15:54:18 2016
Z,enstart64,enstart64,C:\WINDOWS\system32\enstart64.exe,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\efssvc.dll,-101
Mon Apr 18 15:50:45 2016
Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%SystemRo
ot%\system32\IEEtwCollector.exe
/V,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001
Mon Apr 18 15:50:45 2016 Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,,,
Mon Apr 18 15:48:25 2016 Z,MSDTC Bridge 4.0.0.0,,,,,,@comres.dll,-2798
Mon Apr 18 15:48:25 2016 Z,SMSvcHost 4.0.0.0,,,,,,ConfigMgr client agent for task
sequence execution
Mon Apr 18 15:48:25 2016 Z,Windows Workflow Foundation
4.0.0.0,,,,,,@%ProgramFiles%\Windows Defender\MsMpRes.dll,-1176
Mon Apr 18 15:45:34 2016 Z,ac.sharedstore,ActivIdentity Shared Store
Service,"C:\Program Files\Common
Files\ActivIdentity\ac.sharedstore.exe",Own_Process,Auto Start,LocalSystem,Provide
access to the shared store. If this service is stopped or disabled, ActivIdentity
products will not function properly.
Mon Apr 18 15:45:16 2016
Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,,
Mon Apr 18 15:45:08 2016 Z,AdobeFlashPlayerUpdateSvc,Adobe Flash Player Update
Service,C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe,Own_Process,
Manual,LocalSystem,This service keeps your Adobe Flash Player installation up to
date with the latest enhancements and security fixes.
Mon Apr 18 15:44:49 2016 Z,AdobeARMservice,Adobe Acrobat Update Service,"C:\Program
Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe",Own_Process,Auto
Start,LocalSystem,Adobe Acrobat Updater keeps your Adobe software up to date.
Mon Apr 18 15:43:23 2016 Z,ASP.NET_4.0.30319,,,,,,@appmgmts.dll,-3251
Mon Apr 18 15:43:21 2016 Z,ASP.NET,,,,,,@appmgmts.dll,-3251
Mon Apr 18 15:43:18 2016 Z,aspnet_state,ASP.NET State
Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe,Own_Proce
ss,Manual,NT AUTHORITY\NetworkService,Provides support for out-of-process session
states for ASP.NET. If this service is stopped, out-of-process requests will not be
processed. If this service is disabled, any services that explicitly depend on it
Page 134

SYSTEM OUTPUT.txt
will fail to start.
Mon Apr 18 15:43:15 2016 Z,.NET Memory Cache 4.0,,,,,,,
Mon Apr 18 15:43:15 2016
Z,NetMsmqActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelIns
tallRC.dll;-8195,"C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"
-NetMsmqActivator,Share_Process,Disabled,NT
AUTHORITY\NetworkService,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMo
delInstallRC.dll,-8194
Mon Apr 18 15:43:15 2016
Z,NetPipeActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelIns
tallRC.dll;-8197,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,Share
_Process,Disabled,NT
AUTHORITY\LocalService,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll,-8196
Mon Apr 18 15:43:15 2016
Z,NetTcpActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInst
allRC.dll;-8199,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,Share_
Process,Disabled,NT
AUTHORITY\LocalService,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll,-8198
Mon Apr 18 15:43:15 2016
Z,NetTcpPortSharing,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelIn
stallRC.dll;-8201,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,Shar
e_Process,Disabled,NT
AUTHORITY\LocalService,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll,-8200
Mon Apr 18 15:42:19 2016 Z,clr_optimization_v4.0.30319_32,Microsoft .NET Framework
NGEN
v4.0.30319_X86,C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,Own_Proces
s,Auto Start,LocalSystem,Microsoft .NET Framework NGEN
Mon Apr 18 15:42:19 2016 Z,clr_optimization_v4.0.30319_64,Microsoft .NET Framework
NGEN
v4.0.30319_X64,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,Own_Proc
ess,Auto Start,LocalSystem,Microsoft .NET Framework NGEN
Mon Apr 18 15:42:14 2016 Z,.NET CLR Networking 4.0.0.0,,,,,,,
Mon Apr 18 15:42:12 2016 Z,clr_optimization_v2.0.50727_32,Microsoft .NET Framework
NGEN
v2.0.50727_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,Own_Proc
ess,Disabled,LocalSystem,Microsoft .NET Framework NGEN
Mon Apr 18 15:42:12 2016 Z,clr_optimization_v2.0.50727_64,Microsoft .NET Framework
NGEN
v2.0.50727_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,Own_Pr
ocess,Disabled,LocalSystem,Microsoft .NET Framework NGEN
Mon Apr 18 15:37:48 2016 Z,dcdbas,System Management
Driver,system32\DRIVERS\dcdbas64.sys,Kernel
driver,Manual,,@%systemroot%\system32\cscsvc.dll,-201
Mon Apr 18 15:34:47 2016 Z,BthEnum,Bluetooth Enumerator
Service,system32\DRIVERS\BthEnum.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Mon Apr 18 15:34:47 2016 Z,BthPan,Bluetooth Device (Personal Area
Network),system32\DRIVERS\bthpan.sys,Kernel driver,Manual,,Bluetooth Device
(Personal Area Network)
Mon Apr 18 15:34:47 2016 Z,RFCOMM,Bluetooth Device (RFCOMM Protocol
TDI),system32\DRIVERS\rfcomm.sys,Kernel driver,Manual,,Bluetooth Device (RFCOMM
Protocol TDI)
Mon Apr 18 15:34:46 2016 Z,BTHUSB,Bluetooth Radio USB
Driver,System32\Drivers\BTHUSB.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102
Mon Apr 18 15:31:22 2016 Z,CcmExec,SMS Agent
Host,C:\WINDOWS\CCM\CcmExec.exe,Own_Process,Auto Start,LocalSystem,Provides change
and configuration services for computer management systems.
Mon Apr 18 15:31:22 2016 Z,smstsmgr,ConfigMgr Task Sequence
Agent,C:\WINDOWS\CCM\TSManager.exe /service,Own_Process,Manual,LocalSystem,ConfigMgr
Page 135

SYSTEM OUTPUT.txt
client agent for task sequence execution
Mon Apr 18 15:30:46 2016 Z,lppsvc,Microsoft Policy Platform Local
Authority,"C:\Program Files\Microsoft Policy Platform\policyHost.exe"
Files\Microsoft Policy Platform\policyHost.exe"
/service,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\lmhsvc.dll,-102
Mon Apr 18 15:30:46 2016 Z,lppsvc,Microsoft Policy Platform Local,"C:\Program
/service,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\lmhsvc.dll,-102
Mon Apr 18 15:30:13 2016
Z,Netlogon,@%SystemRoot%\system32\netlogon.dll,-102,%systemroot%\system32\lsass.exe,
Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\netlogon.dll,-103
Mon Apr 18 15:30:12 2016 Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own_Process,Manual,LocalSystem,Inte
1(R) Content Protection HECI Service - enables communication with the Content
Protection FW
Mon Apr 18 15:30:12 2016
Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll,-501,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\ikeext.dll,-502
Mon Apr 18 15:29:32 2016
Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll,-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\TabSvc.dll,-101
Mon Apr 18 15:29:32 2016 Z,wlansvc\Parameters,,%SystemrRoot%\system32\wlansvc.dll,,,,
Mon Apr 18 15:29:03 2016 Z,w32time\Parameters,,%systemroot%\system32\w32time.dll,,,,
Mon Apr 18 15:29:01 2016 Z,WinDefend,@%ProgramFiles%\Windows
Defender\MsMpEng.dll,-103,%SystemRoot%\system32\svchost.exe -k
secsvcs,Share_Process,Manual,LocalSystem,@%ProgramFiles%\Windows
Defender\MsMpEng.dll,-1176
Mon Apr 18 15:28:58 2016
Z,{4525A64F-379A-4D68-8A81-DA5AA833E191},,,,,,@%SystemRoot%\system32\wwansvc.dll,-25
8
Mon Apr 18 15:28:54 2016
Z,certpropsvc,@%SystemRoot%\system32\certprop.dll,-11,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\certprop.dll,-12
Mon Apr 18 15:28:54 2016.
Z,scardsvr,@%SystemRoot%\system32\ScardSvr.dll,-1,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\ScardSvr.dll,-5
Mon Apr 18 15:28:51 2016 Z,BTHPORT,Bluetooth Port
Driver,system32\Drivers\BTHport.sys,Kernel driver,Manual,,Bluetooth Device (Personal
Area Network)
Mon Apr 18 15:28:13 2016 Z,MSPQM,Microsoft Streaming Quality Manager
Proxy,system32\drivers\MSPQM.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\msimsg.dll,-32
Mon Apr 18 15:28:13 2016 Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink
Converter,system32\drivers\MSTEE.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\msimsg.dll,-32
Mon Apr 18 15:28:12 2016 Z,MSPCLOCK,Microsoft Streaming Clock
Proxy,system32\drivers\MSPCLOCK.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\msimsg.dll,-32
Mon Apr 18 15:28:07 2016 Z,RtkAudioService,Realtek Audio Service,"C:\Program
Files\Realtek\Audio\HDA\RtkAudioService64.exe",Own_Process,Auto
Start,LocalSystem,For cooperation with Realtek audio driver.
Mon Apr 18 15:28:04 2016
Z,wlansvc,@%SystemRoot%\system32\wlansvc.dll,-257,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\wlansvc.dll,-258
Mon Apr 18 15:28:03 2016
Z,{03302689-7329-415D-8068-DD988B39352S},,,,,,@%SystemRoot%\system32\wwansvc.dll,-25
8
Mon Apr 18 15:28:02 2016
Z,O2FLASH,O2FLASH,%SystemRoot%\system32\DRIVERS\o2flash.exe,Own_Process,Auto
Start,LocalSystem,Provides system and desktop level support to the NVIDIA display
Page 136

SYSTEM OUTPUT.txt

driver
service,"C:\WINDOWS\system32\nvsvc.exe","Own_Process,Auto Start,LocalSystem,Provides
Mon Apr 18 15:28:01 2016 Z,nvsvc,NVIDIA Display Driver
system and desktop level support to the NVIDIA display driver
Files\DellTPad\HidMonitorSvc.exe,Auto Start,LocalSystem,Monitor HID
Mon Apr 18 15:27:42 2016 Z,ApHidMonitorService,Alps HID Monitor Service,C:\Program
device for Alps
Mon Apr 18 15:27:40 2016
z,{4BA4B36E-29B2-45EB-8693-07A52C8F3CC5},,,,,,@%SystemRoot%\system32\wwansvc.dll,-25
8
Mon Apr 18 15:27:22 2016
z,talm,,,,,@%SystemRoot%\system32\drivers\hwpolicy.sys,-102
Mon Apr 18 15:27:21 2016 Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
service,%SystemRoot%\system32\igfxCUIService.exe,Own_Process,Auto
start,LocalSystem,Service for Intel(R) HD Graphics Control Panel
Mon Apr 18 15:26:58 2016 Z,atapi,,\SystemRoot\system32\drivers\atapi.sys,kernel
driver,Manual,,@%SystemRoot%\system32\rascfg.dll,-32000
Mon Apr 18 15:26:58 2016 Z,cdrom,,\SystemRoot\system32\drivers\cdrom.sys,kernel
driver,Manual,,ISO9660/Joliet File System Reader for CD/DVDs. (Core) (All pieces)
Mon Apr 18 15:26:58 2016 Z,HPSAMD,,\SystemRoot\system32\drivers\HPSAMD.sys,kernel
driver,Manual,,@%SystemRoot%\system32\provsvc.dll,-101
Mon Apr 18 15:26:58 2016 Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,kernel
driver,Manual,,@%SystemRoot%\system32\1renum.sys,-101
Mon Apr 18 15:26:58 2016 Z,LSI_SAS,,\SystemRoot\system32\drivers\lsi_sas.sys,kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-201
Mon Apr 18 15:26:58 2016 Z,LSI_SCSI,,\SystemRoot\system32\drivers\lsi_scsi.sys,kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Mon Apr 18 15:26:58 2016 Z,megasR,,\SystemRoot\system32\drivers\megasR.sys,kernel
driver,Manual,,Allows scheduling of McAfee scanning and updating activities.
Mon Apr 18 15:26:58 2016 Z,msahci,,\SystemRoot\system32\drivers\msahci.sys,kernel
driver,Manual,,@%SystemRoot%\system32\wkssvc.dll,-1007
Mon Apr 18 15:26:58 2016 Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,kernel
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Mon Apr 18 15:26:58 2016 Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,kernel
driver,Manual,,@%SystemRoot%\system32\pcasvc.dll,-2
Mon Apr 18 15:26:58 2016
z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,kernel
driver,Manual,,@%SystemRoot%\system32\samsrv.dll,-2
Mon Apr 18 15:26:58 2016 Z,wd,,\SystemRoot\system32\drivers\wd.sys,kernel
driver,Manual,,@%SystemRoot%\system32\wcsPluginService.dll,-201
Mon Apr 18 15:26:57 2016 Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,kernel
driver,Manual,,This service keeps your Adobe Flash Player installation up to date
with the latest enhancements and security fixes.
Mon Apr 18 15:26:57 2016 Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,kernel
driver,Manual,,This service keeps your Adobe Flash Player installation up to date
with the latest enhancements and security fixes.
Mon Apr 18 15:26:57 2016 Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,kernel
driver,Manual,,This service keeps your Adobe Flash Player installation up to date
with the latest enhancements and security fixes.
Mon Apr 18 15:26:57 2016 Z,a1i1de,,\SystemRoot\system32\drivers\a1i1de.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Mon Apr 18 15:26:57 2016 Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Mon Apr 18 15:26:57 2016 Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Mon Apr 18 15:26:57 2016 Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Mon Apr 18 15:26:57 2016 Z,arc,,\SystemRoot\system32\drivers\arc.sys,kernel
driver,Manual,,@appmgmts.dll,-3251
Mon Apr 18 15:26:57 2016 Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,kernel
driver,Manual,,@appmgmts.dll,-3251
Mon Apr 18 15:26:57 2016 Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,kernel

Page 137

SYSTEM OUTPUT.txt
driver,Manual,,Microsoft .NET Framework NGEN
Mon Apr 18 15:26:57 2016 Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\efssvc.dll,-101
Mon Apr 18 15:26:57 2016 Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Mon Apr 18 15:26:57 2016 Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,Kernel
driver,Manual,,Service for Intel(R) HD Graphics Control Panel
Mon Apr 18 15:26:57 2016
Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Mon Apr 18 15:26:57 2016 Z,LSI_FC,,\SystemRoot\system32\drivers\lsi_fc.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Mon Apr 18 15:26:57 2016
Z,LSI_SAS2,,\SystemRoot\system32\drivers\lsi_sas2.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Mon Apr 18 15:26:57 2016 Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,Kernel
driver,Manual,,Allows scheduling of McAfee scanning and updating activities.
Mon Apr 18 15:26:57 2016 Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,Kernel
driver,Manual,,The Mozilla Maintenance Service ensures that you have the latest and
most secure version of Mozilla Firefox on your computer. Keeping Firefox up to date
is very important for your online security, and Mozilla strongly recommends that you
keep this service enabled.
Mon Apr 18 15:26:57 2016 Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,Kernel
driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1007
Mon Apr 18 15:26:57 2016 Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,Kernel
driver,Manual,,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstall
RC.dll,-8200
Mon Apr 18 15:26:57 2016 Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Mon Apr 18 15:26:57 2016 Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\pacer.sys,-101
Mon Apr 18 15:26:57 2016 Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\pacer.sys,-101
Mon Apr 18 15:26:57 2016
Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\shsvcs.dll,-12289
Mon Apr 18 15:26:57 2016
Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\shsvcs.dll,-12289
Mon Apr 18 15:26:57 2016 Z,ST7007,,\SystemRoot\system32\drivers\ST7007.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\sstpsvc.dll,-201
Mon Apr 18 15:26:57 2016
Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\sstpsvc.dll,-201
Mon Apr 18 15:26:57 2016 Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\StorSvc.dll,-101
Mon Apr 18 15:26:57 2016 Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Mon Apr 18 15:26:57 2016 Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,Kernel
driver,Manual,,Cisco AnyConnect Secure Mobility Agent for Windows
Mon Apr 18 15:26:55 2016 Z,TsUsbGD,Remote Desktop Generic USB
Device,\SystemRoot\system32\drivers\TsUsbGD.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Mon Apr 18 15:24:49 2016 Z,bcmnfcusb,NFC USB Bus
Driver,\SystemRoot\system32\drivers\bcmnfcusb7.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\AxInstSV.dll,-104
Mon Apr 18 15:23:49 2016 Z,ISCT,Intel(R) Smart Connect Technology Device
Driver,\SystemRoot\system32\drivers\ISCTD.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Mon Apr 18 15:22:46 2016 Z,iwsehub,Intel(R) WSE Hub
Driver,\SystemRoot\system32\drivers\iwsehub.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Mon Apr 18 15:22:46 2016 Z,iwsepal,Intel(R) WSE-PAL
Page 138

SYSTEM OUTPUT.txt
Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\qmgr.dll,-1001
Wed Dec 30 12:27:20 2015
Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
regsvc,Share_Process,Auto Start,NT AUTHORITY\LocalService,@regsvc.dll,-2
Wed Dec 30 12:27:10 2015
Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.exe
-k bthsvcs,Share_Process,Disabled,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\bthserv.dll,-102
Wed Dec 30 12:26:59 2015
Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Disabled,localSystem,@%SystemRoot%\system32\bdesvc.dll,-101
Wed Dec 30 10:09:44 2015 Z,amdxata,,system32\drivers\amdxata.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\Alg.exe,-113
Wed Dec 30 09:12:34 2015
Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k
WbioSvcGroup,Share_Process,Manual,LocalSystem,@%systemroot%\system32\wbiosrvc.dll,-1
01
Wed Dec 30 07:48:59 2015 Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k
GPSvcGroup,Own_Process,Auto Start,LocalSystem,@gpapi.dll,-113
Wed Dec 30 07:41:07 2015
Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\svch
ost.exe -k utcsvc,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\UtcResources.dll,-3002
Wed Dec 30 07:41:07 2015
Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,,
Wed Dec 30 07:41:07 2015
Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svchost.e
xe -k LocalService,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\FntCache.dll,-101
Wed Dec 30 07:41:07 2015
Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,,
Wed Dec 30 07:41:07 2015 Z,iSCsiPrt,iSCsiPort
Driver,\SystemRoot\system32\drivers\msiscsi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Wed Dec 30 07:41:07 2015 Z,terminpt,Microsoft Remote Desktop Input
Driver,\SystemRoot\system32\drivers\terminpt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\tcpipcfg.dll,-50004
Wed Dec 30 07:41:07 2015 Z,usbcir,eHome Infrared Receiver
(USBCIR),\SystemRoot\system32\drivers\usbcir.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Dec 30 07:41:07 2015
Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wat\Wa
tAdminSvc.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\Wat\WatUX.exe,-6
02
Wed Dec 30 07:41:07 2015
Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\webclnt.dll,-101
Wed Dec 30 07:41:07 2015
Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wudfsvc.dll,-1001
Wed Dec 30 07:03:57 2015 Z,MSDTC Bridge 3.0.0.0,,,,,,@comres.dll,-2798
Wed Dec 30 07:03:57 2015 Z,ServiceModelEndpoint
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Wed Dec 30 07:03:57 2015 Z,ServiceModelOperation
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Wed Dec 30 07:03:57 2015 Z,ServiceModelService
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Wed Dec 30 07:03:57 2015 Z,SMSvcHost 3.0.0.0,,,,,,ConfigMgr client agent for task
Page 140

SYSTEM OUTPUT.txt
sequence execution
Wed Dec 30 07:03:57 2015 Z,Windows Workflow Foundation
3.0.0.0,,,,,,,@%ProgramFiles%\Windows Defender\MsMpRes.dll,-1176
Tue Dec 29 15:55:14 2015 Z,Microsoft SharePoint Workspace Audit Service,Microsoft
SharePoint Workspace Audit Service,"C:\Program Files (x86)\Microsoft
Office\Office14\GROOVE.EXE" /auditservice,Own_Process,Manual,NT
AUTHORITY\LocalService,Provides validation trust protection services
Tue Dec 29 15:55:13 2015 Z,Outlook,,,,,,,Office Software Protection Platform Service
(unlocalized description)
Tue Dec 29 15:55:12 2015 Z,adsi,,,,,,,This service keeps your Adobe Flash Player
installation up to date with the latest enhancements and security fixes.
Tue Dec 29 15:52:10 2015 Z,osppsvc,Office Software Protection Platform,"C:\Program
Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",Own_Process,Manual,NT
AUTHORITY\NetworkService,Office Software Protection Platform Service (unlocalized
description)
Tue Dec 29 15:51:22 2015
Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\wuaueng.dll,-106
Tue Dec 29 15:51:11 2015 Z,ose,Office  Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",Own_Process,Manual,LocalSystem,Saves
installation files used for updates and repairs and is required for the downloading
of Setup updates and Watson error reports.
Tue Apr 12 07:45:41 2011
Z,CscService,@%systemroot%\system32\cscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\cscsvc.dll,-201
Tue Apr 12 07:45:24 2011
Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@appmgmts.dll,-3251
Tue Apr 12 07:45:24 2011
Z,PeerDistSvc,@%SystemRoot%\system32\peerdistsvc.dll;-9000,%SystemRoot%\System32\svc
host.exe -k PeerDist,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\peerdistsvc.dll,-9001
Tue Apr 12 07:45:24 2011 Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100
Tue Apr 12 07:45:24 2011
Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svchost.e
xe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\sensrsvc.dll,-1001
Tue Apr 12 07:45:24 2011
Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\StorSvc.dll,-101
Tue Apr 12 07:45:24 2011
Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%SystemRoot%\system32
\umrdp.dll,-1001
Tue Apr 12 07:45:24 2011, Z,VGPU,,System32\drivers\rdvgkmd.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Tue Apr 12 07:45:22 2011
Z,AppMgmt\Parameters,,%SystemRoot%\System32\appmgmts.dll,,,,
Tue Apr 12 07:45:22 2011
Z,CscService\Parameters,,%SystemRoot%\System32\cscsvc.dll,,,,
Tue Apr 12 07:45:22 2011
Z,PeerDistSvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,,
Tue Apr 12 07:45:22 2011
Z,RDPUDD,,,,,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100
Tue Apr 12 07:45:22 2011
Page 141

SYSTEM OUTPUT.txt

z,sensrsvc\Parameters,,%SystemRoot%\system32\%SystemRoot%\sensrsvc.dll,,,,'
Tue Apr 12 07:45:22 2011 z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,,'
Tue Apr 12 07:45:22 2011 z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,,'
Tue Apr 12 07:44:54 2011 z,dmvsc,,\SystemRoot\system32\drivers\dmvsc.sys,kernel
driver,Manual,,Manages DisplayLink Graphics Adapters according to windows display
properties
Sun Nov 21 03:58:24 2010 z,BTHMODEM,Bluetooth Serial Communications
driver,\SystemRoot\system32\drivers\bthmodem.sys,kernel
driver,Manual,,@%SystemRoot%\system32\browser.dll,-101
Sun Nov 21 03:58:22 2010 z,gagp30kx,Microsoft Generic AGPv3.0 Filter for K8
Processor Platform,\SystemRoot\system32\drivers\gagp30kx.sys,kernel
driver,Manual,,@%SystemRoot%\system32\drivers\fvevol.sys,-100
Sun Nov 21 03:58:22 2010 z,uagp35,Microsoft AGPv3.5
Filter,\SystemRoot\system32\drivers\uagp35.sys,kernel •
driver,Manual,,@%SystemRoot%\system32\drivers\tsushub.sys,-2
Sun Nov 21 03:58:21 2010 z,b06bdrv,Broadcom NetXtreme II
VBD,\SystemRoot\system32\drivers\bxvbda.sys,kernel
driver,Manual,,@%SystemRoot%\system32\AxinstSV.dll,-104
Sun Nov 21 03:58:21 2010 z,HidBth,Microsoft Bluetooth HID
Miniport,\SystemRoot\system32\drivers\hidbth.sys,kernel driver,Manual,,keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:19 2010 z,Amdk8,AMD K8 Processor
Driver,\SystemRoot\system32\drivers\amdk8.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Sun Nov 21 03:58:19 2010 z,AmdPPM,AMD Processor
Driver,\SystemRoot\system32\drivers\amdppm.sys,kernel
driver,Manual,,@%SystemRoot%\system32\A1g.exe,-113
Sun Nov 21 03:58:19 2010 z,Processor,Processor
Driver,\SystemRoot\system32\drivers\processr.sys,kernel
driver,Manual,,@%SystemRoot%\system32\rascfg.dll,-32006
Sun Nov 21 03:58:18 2010 z,ebdrv,Broadcom NetXtreme II 10 GigE
VBD,\SystemRoot\system32\drivers\evbda.sys,kernel
driver,Manual,,@%SystemRoot%\system32\eapsvc.dll,-2
Sun Nov 21 03:58:17 2010 z,pcmcia,,\SystemRoot\system32\drivers\pcmcia.sys,kernel
driver,Manual,,@%SystemRoot%\system32\pcasvc.dll,-2
Sun Nov 21 03:58:16 2010 z,MTConfig,Microsoft Input Configuration
Driver,\SystemRoot\system32\drivers\MTConfig.sys,kernel
driver,Manual,,@%SystemRoot%\system32\msimsg.dll,-32
Sun Nov 21 03:58:15 2010 z,circlass,Consumer IR
Devices,\SystemRoot\system32\drivers\circlass.sys,kernel driver,Manual,,Cisco IP
Communicator driver for CDP
Sun Nov 21 03:58:13 2010 z,sfloppy,High-Capacity Floppy Disk
Drive,\SystemRoot\system32\drivers\sfloppy.sys,kernel
driver,Manual,,@%SystemRoot%\system32\sessenv.dll,-1027
Sun Nov 21 03:58:11 2010 z,HidBatt,HID UPS Battery
Driver,\SystemRoot\system32\drivers\HidBatt.sys,kernel driver,Manual,,keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:08 2010 z,Hidir,Microsoft Infrared HID
Driver,\SystemRoot\system32\drivers\hidir.sys,kernel driver,Manual,,keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:07 2010 z,sermouse,Serial Mouse
Driver,\SystemRoot\system32\drivers\sermouse.sys,kernel
driver,Manual,,@%SystemRoot%\system32\sensrsvc.dll,-1001
Page 142

SYSTEM OUTPUT.txt
Sun Nov 21 03:58:06 2010 Z,BrFiltLo,Brother USB Mass-Storage Lower Filter
Driver,\SystemRoot\system32\drivers\BrFiltLo.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-103
Sun Nov 21 03:58:06 2010 Z,BrFiltUp,Brother USB Mass-Storage Upper Filter
Driver,\SystemRoot\system32\drivers\BrFiltUp.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-103
Sun Nov 21 03:58:05 2010 Z,usbohci,Microsoft USB Open Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbohci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Sun Nov 21 03:58:05 2010 Z,usbuhci,Microsoft USB Universal Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbuhci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Sun Nov 21 03:58:00 2010 Z,WacomPen,Wacom Serial Pen HID
Driver,\SystemRoot\system32\drivers\wacompen.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\w32time.dll,-201
Sun Nov 21 03:57:59 2010 Z,crcdisk,Crcdisk Filter
Driver,\SystemRoot\system32\drivers\crcdisk.sys,Kernel driver,Disabled,,Intel(R)
Content Protection HECI Service - enables communication with the Content Protection
FW
Sun Nov 21 03:57:58 2010 Z,UmPass,Microsoft UMPass
Driver,\SystemRoot\system32\drivers\umpass.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102
Sun Nov 21 03:57:56 2010 Z,usbprint,Microsoft USB PRINTER
Class,\SystemRoot\system32\drivers\usbprint.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Sun Nov 21 03:46:56 2010 Z,b57nd60a,Broadcom NetXtreme Gigabit Ethernet - NDIS
6.0,system32\DRIVERS\b57nd60a.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\AxInstSV.dll,-104
Sun Nov 21 03:46:56 2010 Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,File system driver,Disabled,,ISO9660/Joliet File
System Reader for CD/DVDs. (Core) (All pieces)
Sun Nov 21 03:46:56 2010 Z,fastfat,FAT12/16/32 File System Driver,,File system
driver,Manual,,Note - dependance on CDROM.SYS only if required to read/write DVD-RAM
media (which appears as CD class device). (Core) (All pieces)
Sun Nov 21 03:46:56 2010 Z,vga,,system32\DRIVERS\vgapnp.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Sun Nov 21 03:39:53 2010 Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,,
Sun Nov 21 03:38:46 2010 Z,TsUsbFlt,,system32\drivers\tsusbflt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Sun Nov 21 03:33:56 2010
Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svchost.
exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,1394ohci,1394 OHCI Compliant Host
Controller,\SystemRoot\system32\drivers\1394ohci.sys,Kernel driver,Manual,,
Sun Nov 21 03:29:32 2010 Z,AcpiPmi,ACPI Power Meter
Driver,\SystemRoot\system32\drivers\acpipmi.sys,Kernel driver,Manual,,Provide access
to the shared store. If this service is stopped or disabled, ActivIdentity products
will not function properly.
Sun Nov 21 03:29:32 2010 Z,agp440,Intel AGP Bus
Filter,\SystemRoot\system32\drivers\agp440.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\afd.sys,-1000
Sun Nov 21 03:29:32 2010 Z,ErrDev,Microsoft Hardware Error Device
Driver,\SystemRoot\system32\drivers\errdev.sys,Kernel driver,Manual,,Host-based
intrusion prevention component that blocks exploits and hacks in real-time,
including malicious buffer overflow code execution and privilege escalations. If
this service is disabled or stopped, the system is no longer protected against
intrusions.
Sun Nov 21 03:29:32 2010 Z,IPMIDRV,,\SystemRoot\system32\drivers\IPMIDrv.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\iphlpsvc.dll,-501
Sun Nov 21 03:29:32 2010 Z,nv_agp,NVIDIA nForce AGP Bus
Filter,\SystemRoot\system32\drivers\nv_agp.sys,Kernel driver,Manual,,Provides system
and desktop level support to the NVIDIA display driver
Page 143

SYSTEM OUTPUT.txt
Sun Nov 21 03:29:32 2010 Z,ohci1394,1394 OHCI Compliant Host Controller
(Legacy),\SystemRoot\system32\drivers\ohci1394.sys,Kernel driver,Manual,,Provides
system and desktop level support to the NVIDIA display driver
Sun Nov 21 03:29:32 2010 Z,sffdisk,SFF Storage Class
Driver,\SystemRoot\system32\drivers\sffdisk.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,sffp_mmc,SFF Storage Protocol Driver for
MMC,\SystemRoot\system32\drivers\sffp_mmc.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,sffp_sd,SFF Storage Protocol Driver for
SDBus,\SystemRoot\system32\drivers\sffp_sd.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,uliagpkx,Uli AGP Bus
Filter,\SystemRoot\system32\drivers\uliagpkx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102
Sun Nov 21 03:29:32 2010 Z,vhdmp,,\SystemRoot\system32\drivers\vhdmp.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Tue Jul 14 05:34:12 2009 Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,,
Tue Jul 14 05:34:12 2009
Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,,
Tue Jul 14 05:34:12 2009 Z,WPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,,
Tue Jul 14 05:34:09 2009
Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,,
Tue Jul 14 05:34:09 2009 Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,,
Tue Jul 14 05:34:09 2009 Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,,
Tue Jul 14 05:08:55 2009
Z,iphlpsvc\Parameters,,%SystemRoot%\System32\iphlpsvc.dll,,,,
Tue Jul 14 04:54:38 2009 Z,NdisCap,NDIS Capture LightWeight
Filter,system32\DRIVERS\ndiscap.sys,Kernel driver,Manual,,NDIS Capture LightWeight
Filter
Tue Jul 14 04:54:32 2009 Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,,
Tue Jul 14 04:54:31 2009
Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,,
Tue Jul 14 04:54:25 2009
Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,,
Tue Jul 14 04:54:05 2009 Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,,
Tue Jul 14 04:53:57 2009
Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\tcpipcfg.dll,-50006
Tue Jul 14 04:53:56 2009 Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,,
Tue Jul 14 04:53:48 2009
Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcss.dll,,,,
Tue Jul 14 04:53:45 2009
Z,Trkwks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\trkwks.dll,-2
Tue Jul 14 04:53:45 2009 Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,,
Tue Jul 14 04:53:36 2009
Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svchost.e
xe -k RPCSS,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%windir%\system32\RpcEpMap.dll,-1002
Tue Jul 14 04:53:36 2009
Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,,
Tue Jul 14 04:53:33 2009
Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\srvsvc.dll,-101
Tue Jul 14 04:53:31 2009
Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32\svc
host.exe -k NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%systemroot%\system32\wkssvc.dll,-101
Tue Jul 14 04:53:31 2009
Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,,
Page 144

SYSTEM OUTPUT.txt

Tue Jul 14 04:53:25 2009 Z,WmiApRpl,,,,,,,@%SystemRoot%\System32\wlansvc.dll,-258
Tue Jul 14 04:53:24 2009
Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,localSystem,@%Systemroot%\system32\wbem\wmisvc.dll,-204
Tue Jul 14 04:53:24 2009
Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\wbem\
WmiApSrv.exe,Own_Process,Manual,localSystem,@%Systemroot%\system32\wbem\wmiapsrv.exe
,-111
Tue Jul 14 04:53:21 2009 Z,TCPIP6,Microsoft IPv6 Protocol
Driver,system32\DRIVERS\tcpip.sys,Kernel driver,Manual,,Microsoft IPv6 Protocol
Driver
Tue Jul 14 04:53:21 2009
Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32011
Tue Jul 14 04:53:20 2009
Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\lmhsvc.dll,-102
Tue Jul 14 04:53:19 2009
Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\dhcpcore.dll,-101
Tue Jul 14 04:53:19 2009
Z,Winsock,,,Adapter,Manual,,@%Systemroot%\system32\wsmsvc.dll,-102
Tue Jul 14 04:49:48 2009
Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Share_P
rocess,Auto Start,LocalSystem,@%SystemRoot%\system32\samsrv.dll,-2
Tue Jul 14 04:49:48 2009
Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\w32time.dll,-201
Tue Jul 14 04:49:46 2009
Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.exe
-k NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\dnsapi.dll,-102
Tue Jul 14 04:49:45 2009
Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svchost.
exe -k
netsvcs,Share_Process,Disabled,localSystem,@%Systemroot%\system32\mprdim.dll,-201
Tue Jul 14 04:49:45 2009
Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,,
Tue Jul 14 04:49:35 2009
Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasauto.dll,-201
Tue Jul 14 04:49:35 2009 Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,,
Tue Jul 14 04:49:35 2009
Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasmans.dll,-201
Tue Jul 14 04:49:26 2009 Z,SstpSvc\Parameters,,%SystemRoot%\System32\sstpsvc.dll,,,,
Tue Jul 14 04:49:24 2009
Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\dps.dll,-501
Tue Jul 14 04:49:24 2009 Z,DPS\Parameters,,%SystemRoot%\System32\dps.dll,,,,
Tue Jul 14 04:49:24 2009
Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svchost.e
xe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\wdi.dll,-503
Tue Jul 14 04:49:24 2009
Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,,
Tue Jul 14 04:49:24 2009
Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchost.ex

Page 145

SYSTEM OUTPUT.txt
e -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\wdi.dll,-501
Tue Jul 14 04:49:24 2009
Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,,
Tue Jul 14 04:49:23 2009 Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,,
Tue Jul 14 04:49:22 2009 Z,TBS\Parameters,,%SystemRoot%\System32\tbssvc.dll,,,,
Tue Jul 14 04:49:20 2009 Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,,
Tue Jul 14 04:49:20 2009 Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,,
Tue Jul 14 04:49:18 2009 Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,,
Tue Jul 14 04:49:08 2009 Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,.NET CLR Data,,,,,,
Tue Jul 14 04:49:01 2009 Z,.NET CLR Networking,,,,,,
Tue Jul 14 04:49:01 2009 Z,.NET Data Provider for Oracle,,,,,,
Tue Jul 14 04:49:01 2009 Z,.NET Data Provider for SqlServer,,,,,,
Tue Jul 14 04:49:01 2009 Z,.NETFramework,,,,,,
Tue Jul 14 04:49:01 2009
Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svchost.e
xe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\system32\aelupsvc.dll,-2
Tue Jul 14 04:49:01 2009
Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own_Process,
Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\Alg.exe,-113
Tue Jul 14 04:49:01 2009
Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\appid.
sys,Kernel driver,Manual,,@%systemroot%\system32\appidsvc.dll,-103
Tue Jul 14 04:49:01 2009
Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
Authority\LocalService,@%systemroot%\system32\appidsvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\appinfo.dll,-101
Tue Jul 14 04:49:01 2009 Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,,
Tue Jul 14 04:49:01 2009
Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\audiosrv.dll,-205
Tue Jul 14 04:49:01 2009
Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\audiosrv.dll,-201
Tue Jul 14 04:49:01 2009
Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchost.ex
e -k
AxInstSVGroup,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\AxInstSV.dll,-
104
Tue Jul 14 04:49:01 2009
Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,,
Tue Jul 14 04:49:01 2009 Z,BattC,,,,,,@%SystemRoot%\system32\AxInstSV.dll,-104
Tue Jul 14 04:49:01 2009
Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\bfe.dll,-1002
Tue Jul 14 04:49:01 2009 Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,,
Page 146

SYSTEM OUTPUT.txt

Tue Jul 14 04:49:01 2009 Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,,
Tue Jul 14 04:49:01 2009 Z,Brserid,Brother MFC Serial Port Interface Driver
(WDM),\SystemRoot\System32\Drivers\Brserid.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Tue Jul 14 04:49:01 2009 Z,BrSerWdm,Brother WDM Serial
driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Tue Jul 14 04:49:01 2009 Z,BrUsbMdm,Brother MFC USB Fax Only
Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Tue Jul 14 04:49:01 2009 Z,BrUsbSer,Brother MFC USB Serial WDM
Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Tue Jul 14 04:49:01 2009 Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,
Tue Jul 14 04:49:01 2009
Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own_Process,Manual,LocalSystem,@co
mres.dll,-948
Tue Jul 14 04:49:01 2009 Z,crypt32,,,,,,Intel(R) Content Protection HECI Service -
enables communication with the Content Protection FW
Tue Jul 14 04:49:01 2009
Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svchost.e
xe -k NetworkService,Share_Process,Auto Start,NT
Authority\NetworkService,@%SystemRoot%\system32\cryptsvc.dll,-1002
Tue Jul 14 04:49:01 2009
Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,DCLocator,,,,,,@%systemroot%\system32\cscsvc.dll,-201
Tue Jul 14 04:49:01 2009
Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem,@oleres.dll,-5013
Tue Jul 14 04:49:01 2009
Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svchost.
exe -k
defragsvc,Own_Process,Manual,localSystem,@%SystemRoot%\system32\defragsvc.dll,-102
Tue Jul 14 04:49:01 2009
Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%systemroot%\system32
\dot3svc.dll,-1103
Tue Jul 14 04:49:01 2009 Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Share_P
rocess,Manual,LocalSystem,@%SystemRoot%\system32\efssvc.dll,-101
Tue Jul 14 04:49:01 2009 Z,ESENT,,,,,,Host-based intrusion prevention component that
blocks exploits and hacks in real-time, including malicious buffer overflow code
execution and privilege escalations. If this service is disabled or stopped, the
system is no longer protected against intrusions.
Tue Jul 14 04:49:01 2009
Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService,@comres.dll,-2451
Tue Jul 14 04:49:01 2009 Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,,
Tue Jul 14 04:49:01 2009 Z,exfat,exFAT File System Driver,,File system
driver,Manual,,exFAT File System Driver
Tue Jul 14 04:49:01 2009
Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\fdPHost.dll,-101
Tue Jul 14 04:49:01 2009 Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,,
Tue Jul 14 04:49:01 2009
Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,,
Tue Jul 14 04:49:01 2009

Page 147

SYSTEM OUTPUT.txt
Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers\fil
etrace.sys,File system
driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000
Tue Jul 14 04:49:01 2009
Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot%\Mi
crosoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\PresentationHost.exe,-3310
Tue Jul 14 04:49:01 2009
Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers\FsD
epends.sys,File system
driver,Manual,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000
Tue Jul 14 04:49:01 2009 Z,hcw85cir,Hauppauge Consumer Infrared
Receiver,\SystemRoot\system32\drivers\hcw85cir.sys,Kernel driver,Manual,,Keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Tue Jul 14 04:49:01 2009
Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\hidserv.dll,-102
Tue Jul 14 04:49:01 2009 Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\kmsvc.dll,-7
Tue Jul 14 04:49:01 2009
Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v
3.0\Windows Communication
Foundation\infocard.exe",Share_Process,Manual,LocalSystem,@%systemroot%\Microsoft.NE
T\Framework64\v3.0\Windows Communication Foundation\ServiceModelInstallRC.dll,-8192
Tue Jul 14 04:49:01 2009 Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,,
Tue Jul 14 04:49:01 2009 Z,inetaccs,,,,,,@%SystemRoot%\system32\ikeext.dll,-502
Tue Jul 14 04:49:01 2009
Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\IPBusEnum.dll,-103
Tue Jul 14 04:49:01 2009
Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,,,
Tue Jul 14 04:49:01 2009
Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipfltdrv.
sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32013
Tue Jul 14 04:49:01 2009
Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchost.ex
e -k NetSvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\iphlpsvc.dll,-501
Tue Jul 14 04:49:01 2009 Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\iphlpsvc.dll,-501
Tue Jul 14 04:49:01 2009
Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.sys,
Kernel driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Tue Jul 14 04:49:01 2009
Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share_Process,Manual,Local
System,@keyiso.dll,-101
Tue Jul 14 04:49:01 2009 Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,Share_Process,Manual,NT
Page 148

SYSTEM OUTPUT.txt
AUTHORITY\NetworkService,@comres.dll,-2947
Tue Jul 14 04:49:01 2009 Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,,
Tue Jul 14 04:49:01 2009 Z,ldap,,,,,,@%systemroot%\system32\wkssvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\lltdres.dll,-2
Tue Jul 14 04:49:01 2009 Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,Lsa,,,,,,@%SystemRoot%\system32\lmhsvc.dll,-102
Tue Jul 14 04:49:01 2009
Z,MMCSS,@%systemroot%\system32\mmcss.dll;-100,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%systemroot%\system32\mmcss.dll,-101
Tue Jul 14 04:49:01 2009 Z,MMCSS\Parameters,,%SystemRoot%\System32\mmcss.dll,,,,
Tue Jul 14 04:49:01 2009 Z,Modem,,system32\drivers\modem.sys,Kernel
driver,Manual,,@%systemroot%\system32\mmcss.dll,-101
Tue Jul 14 04:49:01 2009
Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svchost
.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\FirewallAPI.dll,-23091
Tue Jul 14 04:49:01 2009 Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System32\d
rivers\mshidkmdf.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mshidkmdf.sys,-101
Tue Jul 14 04:49:01 2009
Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchost.ex
e -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\iscsidsc.dll,-5001
Tue Jul 14 04:49:01 2009
Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,,
Tue Jul 14 04:49:01 2009
Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.exe
/V,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\msimsg.dll,-32
Tue Jul 14 04:49:01 2009 Z,MsRPC,,,Kernel
driver,Manual,,@%SystemRoot%\system32\msimsg.dll,-32
Tue Jul 14 04:49:01 2009 Z,MSSCNTRS,,,,,,@%SystemRoot%\system32\msimsg.dll,-32
Tue Jul 14 04:49:01 2009
Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\qagentrt.dll,-7
Tue Jul 14 04:49:01 2009
Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\netman.dll,-110
Tue Jul 14 04:49:01 2009 Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,,
Tue Jul 14 04:49:01 2009
Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchost.ex
e -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\netprofm.dll,-203
Tue Jul 14 04:49:01 2009
Z,netprofm\Parameters,,%SystemRoot%\System32\netprofm.dll,,,,
Tue Jul 14 04:49:01 2009
Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\nlasvc.dll,-2
Tue Jul 14 04:49:01 2009
Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\nsisvc.dll,-201
Tue Jul 14 04:49:01 2009 Z,NTDS,,,,,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Tue Jul 14 04:49:01 2009
Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchost.ex
e -k LocalServicePeerNet,Share_Process,Manual,NT
Page 149

SYSTEM OUTPUT.txt
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8005
Tue Jul 14 04:49:01 2009
Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\p2psvc.dll,-8007
Tue Jul 14 04:49:01 2009
Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\pcasvc.dll,-2
Tue Jul 14 04:49:01 2009 Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,PerfDisk,,,,,,@%SystemRoot%\system32\peerdistsvc.dll,-9001
Tue Jul 14 04:49:01 2009
Z,PerfHost,@%systemroot%\syswow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost.exe
,Own_Process,Manual,NT AUTHORITY\LocalService,@%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfNet,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfOS,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfProc,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009
Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\pla.dll,-501
Tue Jul 14 04:49:01 2009 Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,,
Tue Jul 14 04:49:01 2009
Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchost.ex
e -k DcomLaunch,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\umpnpmgr.dll,-101
Tue Jul 14 04:49:01 2009
Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpauto.dll,-8003
Tue Jul 14 04:49:01 2009
Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8001
Tue Jul 14 04:49:01 2009 Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\svchos
t.exe -k NetworkServiceNetworkRestricted,Share_Process,Manual,NT
Authority\NetworkService,@%SystemRoot%\system32\polstore.dll,-5011
Tue Jul 14 04:49:01 2009
Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,PortProxy,,,,,,@%SystemRoot%\system32\polstore.dll,-5011
Tue Jul 14 04:49:01 2009
Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\umpo.dll,-101
Tue Jul 14 04:49:01 2009 Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\profsvc.dll,-301
Tue Jul 14 04:49:01 2009 Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ProtectedStorage,@%systemroot%\system32\psbase.dll;-300,%SystemRoot%\system32\lsas
s.exe,Share_Process,Manual,LocalSystem,@%systemroot%\system32\psbase.dll,-301
Tue Jul 14 04:49:01 2009
Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\qwave.dll,-2
Tue Jul 14 04:49:01 2009 Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,,
Tue Jul 14 04:49:01 2009
Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\drive
rs\qwavedrv.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\qwavedrv.sys,-2
Page 150

SYSTEM OUTPUT.txt
Tue Jul 14 04:49:01 2009 Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,Kernel driver,Manual,,Remote Access Auto
Connection Driver
Tue Jul 14 04:49:01 2009 Z,RDPDD,,,,,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101
Tue Jul 14 04:49:01 2009
Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,,,@%systemroot%\system32\drprov.dll
,-101
Tue Jul 14 04:49:01 2009
Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator.exe
,Own_Process,Manual,NT
AUTHORITY\NetworkService,@%systemroot%\system32\Locator.exe,-3
Tue Jul 14 04:49:01 2009 Z,RpcSs,@oleres.dll;-5010,%SystemRoot%\system32\svchost.exe
-k rpcss,Share_Process,Auto Start,NT AUTHORITY\NetworkService,@oleres.dll,-5011
Tue Jul 14 04:49:01 2009
Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchost.ex
e -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\schedsvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svchost.
exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\certprop.dll,-14
Tue Jul 14 04:49:01 2009
Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.exe -k
SDRSVC,Own_Process,Manual,localSystem,@%SystemRoot%\system32\sdrsvc.dll,-102
Tue Jul 14 04:49:01 2009
Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.exe
-k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\seclogon.dll,-7000
Tue Jul 14 04:49:01 2009 Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\Sens.dll,-201
Tue Jul 14 04:49:01 2009 Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\svchos
t.exe -k
netsvcs,Share_Process,Disabled,LocalSystem,@%SystemRoot%\system32\ipnathlp.dll,-107
Tue Jul 14 04:49:01 2009
Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\shsvcs.dll,-12289
Tue Jul 14 04:49:01 2009
Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap.exe
,Own_Process,Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\snmptrap.exe,-4
Tue Jul 14 04:49:01 2009
Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.exe,Ow
n_Process,Auto Start,LocalSystem,@%systemroot%\system32\spoolsv.exe,-2
Tue Jul 14 04:49:01 2009
Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe,Own
Page 151

SYSTEM OUTPUT.txt

```
_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\sppsvc.exe,-100
Tue Jul 14 04:49:01 2009
Z,sppuinotify,@%SystemRoot%\system32\sppuinotify.dll;-103,%SystemRoot%\system32\svch
ost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\sppuinotify.dll,-102
Tue Jul 14 04:49:01 2009
Z,sppuinotify\Parameters,,%SystemRoot%\system32\sppuinotify.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\ssdpsrv.dll,-101
Tue Jul 14 04:49:01 2009 Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\sstpsvc.dll,-201
Tue Jul 14 04:49:01 2009
Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.exe -k
imgsvc,Own_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\wiaservc.dll,-10
Tue Jul 14 04:49:01 2009 Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe -k
swprv,Own_Process,Manual,LocalSystem,@%SystemRoot%\System32\swprv.dll,-102
Tue Jul 14 04:49:01 2009 Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\sysmain.dll,-1001
Tue Jul 14 04:49:01 2009 Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,,
Tue Jul 14 04:49:01 2009
Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchost.ex
e -k NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\tapisrv.dll,-10101
Tue Jul 14 04:49:01 2009 Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,TBS,@%SystemRoot%\system32\tbssvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\tbssvc.dll,-101
Tue Jul 14 04:49:01 2009 Z,TCPIP6TUNNEL,,,,,,Microsoft IPv6 Protocol Driver
Tue Jul 14 04:49:01 2009 Z,TCPIPTUNNEL,,,,,,Provides compatibility for legacy
applications which interact with TCP/IP through the registry. If this service is
stopped, certain applications may have impaired functionality.
Tue Jul 14 04:49:01 2009 Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,Kernel
driver,Manual,,Provides compatibility for legacy applications which interact with
TCP/IP through the registry. If this service is stopped, certain applications may
have impaired functionality.
Tue Jul 14 04:49:01 2009
Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svchost.
exe -k NetworkService,Share_Process,Manual,NT
Authority\NetworkService,@%SystemRoot%\System32\termsrv.dll,-267
Tue Jul 14 04:49:01 2009
Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svchost
.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\themeservice.dll,-8193
Tue Jul 14 04:49:01 2009
Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,,
Tue Jul 14 04:49:01 2009
```

Page 152

SYSTEM OUTPUT.txt

Z,THREADORDER,@%systemroot%\system32\mmcss.dll;-102,%SystemRoot%\system32\svchost.ex
e -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\mmcss.dll,-103
Tue Jul 14 04:49:01 2009
Z,TSDDD,,,,,,@%SystemRoot%\servicing\TrustedInstaller.exe,-101
Tue Jul 14 04:49:01 2009 Z,UGatherer,,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc
formats, usually found on C/DVD discs. (Core) (All pieces)
Tue Jul 14 04:49:01 2009 Z,UGTHRSVC,,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc
formats, usually found on C/DVD discs. (Core) (All pieces)
Tue Jul 14 04:49:01 2009
Z,UIODetect,@%SystemRoot%\system32\ui0detect.exe;-101,%SystemRoot%\system32\UIODetec
t.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\ui0detect.exe,-102
Tue Jul 14 04:49:01 2009
Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\upnphost.dll,-214
Tue Jul 14 04:49:01 2009
Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,,
Tue Jul 14 04:49:01 2009
Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,localSystem,@%SystemRoot%\system32\dwm.exe,-2001
Tue Jul 14 04:49:01 2009 Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,,
Tue Jul 14 04:49:01 2009
Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass.exe
,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\vaultsvc.dll,-1004
Tue Jul 14 04:49:01 2009
Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Process,
Manual,LocalSystem,@%SystemRoot%\system32\vds.exe,-112
Tue Jul 14 04:49:01 2009
Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_Proc
ess,Manual,LocalSystem,@%systemroot%\system32\vssvc.exe,-101
Tue Jul 14 04:49:01 2009 Z,W3SVC,,,,,,@%SystemRoot%\system32\w32time.dll,-201
Tue Jul 14 04:49:01 2009
Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbengine.
exe",Own_Process,Manual,localSystem,@%systemroot%\system32\wbengine.exe,-105
Tue Jul 14 04:49:01 2009
Z,WbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\wcncsvc.dll,-4
Tue Jul 14 04:49:01 2009 Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%\sys
tem32\svchost.exe -k wcssvc,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\WcsPlugInService.dll,-201
Tue Jul 14 04:49:01 2009
Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\wecsvc.dll,-201
Tue Jul 14 04:49:01 2009 Z,Wecsvc\Parameters,,%SystemRoot%\System32\wecsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\System32\
svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\wercplsupport.dll,-1
00
Tue Jul 14 04:49:01 2009
Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
Page 153

SYSTEM OUTPUT.txt
WerSvcGroup,Share_Process,Manual,localSystem,@%SystemRoot%\System32\wersvc.dll,-101
Tue Jul 14 04:49:01 2009 Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,File
system driver,Manual,,WIM Image mount service driver
Tue Jul 14 04:49:01 2009 Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\system32\
svchost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\winhttp.dll,-101
Tue Jul 14 04:49:01 2009
Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%Systemroot%\system32\wsmsvc.dll,-102
Tue Jul 14 04:49:01 2009 Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,WinSock2,,,,,,@%Systemroot%\system32\wsmsvc.dll,-102
Tue Jul 14 04:49:01 2009 Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe",Own_Process,Manual,NT
AUTHORITY\NetworkService,@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102
Tue Jul 14 04:49:01 2009
Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\svchos
t.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wpdbusenum.dll,-101
Tue Jul 14 04:49:01 2009
Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\driv
ers\ws2ifsl.sys,Kernel
driver,Disabled,,@%systemroot%\System32\drivers\ws2ifsl.sys,-1000
Tue Jul 14 04:49:01 2009
Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\wscsvc.dll,-201
Tue Jul 14 04:49:01 2009 Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WSearchIdxPi,,,,,,@%systemroot%\system32\SearchIndexer.exe,-104
Tue Jul 14 04:49:01 2009
Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,,
Tue Jul 14 04:49:01 2009 Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.exe
-k LocalServiceNoNetwork,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 04:49:01 2009 Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,xmlprov,,,,,,@%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 02:34:41 2009
Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,
Tue Jul 14 02:34:41 2009 Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,
-----------------------------------------
Thu Apr 28 15:00:49 2016Z,mferkdet,McAfee Inc.
mferkdet,system32\drivers\mferkdet.sys,Kernel driver,Manual,
Thu Apr 28 15:00:38 2016Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,
Thu Apr 28 15:00:36 2016Z,mfeapfk,McAfee Inc.
mfeapfk,system32\drivers\mfeapfk.sys,Kernel driver,Manual,
Wed Apr 20 15:58:48
2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot
%\servicing\TrustedInstaller.exe,Own_Process,Manual,localSystem
Wed Apr 20 15:42:05 2016Z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,Kernel driver,Boot Start,
Wed Apr 20 15:42:04 2016Z,DisplayLinkService,DisplayLinkManager,"C:\Program
Files\DisplayLink Core Software\DisplayLinkManager.exe",272,Auto Start,LocalSystem
Page 154

SYSTEM OUTPUT.txt

Wed Apr 20 15:41:02
2016Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asyncmac.sys,Kernel driver,Manual,
Wed Apr 20 15:40:59
2016Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,
Wed Apr 20 15:40:59 2016Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,Kernel driver,Manual,
Wed Apr 20 15:40:59 2016Z,mfeavfk01,McAfee Inc.,,Kernel driver,Manual,
Wed Apr 20 15:40:59 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common Files\McAfee\SystemCore\\mfemms.exe",Own_Process,Auto Start,LocalSystem
Wed Apr 20 15:40:59 2016Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Wed Apr 20 15:40:59
2016Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,
Wed Apr 20 15:40:52 2016Z,cvusbdrv,Dell
ControlVault,System32\Drivers\cvusbdrv.sys,Kernel driver,Manual,
Wed Apr 20 15:40:52 2016Z,kbdhid,Keyboard HID
Driver,system32\DRIVERS\kbdhid.sys,Kernel driver,Manual,
Wed Apr 20 15:40:52 2016Z,mouhid,Mouse HID Driver,system32\DRIVERS\mouhid.sys,Kernel driver,Manual,
Wed Apr 20 15:40:52
2016Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfilter.sys,Kernel driver,Manual,
Wed Apr 20 15:40:52 2016Z,WinUsb,WinUSB Driver,system32\DRIVERS\WinUSB.sys,Kernel driver,Manual,
Wed Apr 20 15:40:51 2016Z,HidUsb,Microsoft HID Class
Driver,system32\DRIVERS\hidusb.sys,Kernel driver,Manual,
Wed Apr 20 15:40:51 2016Z,monitor,Microsoft Monitor Class Function Driver
Service,system32\DRIVERS\monitor.sys,Kernel driver,Manual,
Wed Apr 20 15:40:51 2016Z,usbccgp,Microsoft USB Generic Parent
Driver,system32\DRIVERS\usbccgp.sys,Kernel driver,Manual,
Wed Apr 20 15:40:51 2016Z,usbvideo,USB Video Device
(WDM),System32\Drivers\usbvideo.sys,Kernel driver,Manual,
Wed Apr 20 15:40:50 2016Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,
Wed Apr 20 15:40:49 2016Z,IntcAzAudAddService,Service for Realtek HD Audio
(WDM),system32\drivers\RTDVHD64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:49 2016Z,iusb3hub,Intel(R) USB 3.0 Hub
Driver,system32\DRIVERS\iusb3hub.sys,Kernel driver,Manual,
Wed Apr 20 15:40:49 2016Z,ST_Accel,STMicroelectronics Accelerometer
Service,system32\DRIVERS\ST_Accel.sys,Kernel driver,Manual,
Wed Apr 20 15:40:48 2016Z,IntcDAud,Intel(R) Display
Audio,system32\DRIVERS\IntcDAud.sys,Kernel driver,Manual,
Wed Apr 20 15:40:48 2016Z,ksthunk,Kernel Streaming
Thunks,\SystemRoot\system32\drivers\ksthunk.sys,Kernel driver,Manual,
Wed Apr 20 15:40:48 2016Z,Parport,Parallel port
driver,system32\DRIVERS\parport.sys,Kernel driver,Manual,
Wed Apr 20 15:40:48 2016Z,usbhub,Microsoft USB Standard Hub
Driver,system32\DRIVERS\usbhub.sys,Kernel driver,Manual,
Wed Apr 20 15:40:47 2016Z,mssmbios,Microsoft System Management BIOS
Driver,system32\DRIVERS\mssmbios.sys,Kernel driver,System Start,
Wed Apr 20 15:40:46 2016Z,nvlddmkm,,system32\DRIVERS\nvlddmkm.sys,Kernel driver,Manual,
Wed Apr 20 15:40:46 2016Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,ACPI,Microsoft ACPI
Driver,system32\drivers\ACPI.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,acsock,acsock,system32\DRIVERS\acsock64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\afd.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,ApfiltrService,Alps Touch Pad Filter Driver for Windows x64,system32\DRIVERS\Apfiltr.sys,Kernel driver,Manual,

Page 155

SYSTEM OUTPUT.txt
Wed Apr 20 15:40:45 2016Z,Beep,Beep,,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,blbdrive,,system32\DRIVERS\blbdrive.sys,Kernel
driver,System Start,
Wed Apr 20 15:40:45
2016Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,Fil
e system driver,Manual,
Wed Apr 20 15:40:45 2016Z,CipcCdp,Cisco IP Communicator driver for
CDP,system32\DRIVERS\CipcCdp.sys,Kernel driver,Auto Start,
Wed Apr 20 15:40:45
2016Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,System32\CLFS.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,CmBatt,Microsoft ACPI Control Method Battery
Driver,system32\DRIVERS\CmBatt.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,Compbatt,Microsoft Composite Battery
Driver,system32\DRIVERS\compbatt.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,CompositeBus,Composite Bus Enumerator
Driver,system32\DRIVERS\CompositeBus.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,CSC,@%systemroot%\system32\cscsvc.dll;-202,system32\drivers\csc.sys,Kernel
driver,System Start,
Wed Apr 20 15:40:45 2016Z,ctxusbm,Citrix USB Monitor
Driver,system32\DRIVERS\ctxusbm.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,CVirtA,Cisco Systems VPN Adapter for 64-bit
Windows,system32\DRIVERS\CVirtA64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,CVPNDRVA,Cisco Systems Inc. IPSec
Driver,\??\C:\WINDOWS\system32\Drivers\CVPNDRVA.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,DfsC,@%systemroot%\system32\drivers\dfsc.sys;-101,System32\Drivers\dfsc.sys,Fi
le system driver,System Start,
Wed Apr 20 15:40:45
2016Z,discache,@%systemroot%\system32\drivers\discache.sys;-102,System32\drivers\dis
cache.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,Disk,Disk Driver,system32\drivers\disk.sys,Kernel
driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,DNE,Deterministic Network Enhancer
Miniport,system32\DRIVERS\dne64x.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,dptf_acpi,,system32\DRIVERS\dptf_acpi.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45 2016Z,dptf_cpu,,system32\DRIVERS\dptf_cpu.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45 2016Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,e1dexpress,Intel(R) PRO/1000 PCI Express Network
Connection Driver D,system32\DRIVERS\e1d62x64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,enstart64_,enstart64_,\??\C:\WINDOWS\system32\enstart64_.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45 2016Z,esif_lf,,system32\DRIVERS\esif_lf.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45
2016Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,system32\drivers\fil
einfo.sys,File system driver,Boot Start,
Wed Apr 20 15:40:45
2016Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmg
r.sys,File system driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,Fs_Rec,,,8,Boot Start,
Wed Apr 20 15:40:45
2016Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.
sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,HDAudBus,Microsoft UAA Bus Driver for High Definition
Audio,system32\DRIVERS\HDAudBus.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
Page 156

SYSTEM OUTPUT.txt
2016Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,Kern
el driver,Manual,
Wed Apr 20 15:40:45
2016Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwp
olicy.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,i8042prt,i8042 Keyboard and PS/2 Mouse Port
Driver,system32\DRIVERS\i8042prt.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,iaStorA,,system32\drivers\iaStorA.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,iaStorF,,system32\drivers\iaStorF.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,igfx,,system32\DRIVERS\igdkmd64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,intelppm,Intel Processor
Driver,system32\DRIVERS\intelppm.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,iusb3xhc,Intel(R) USB 3.0 eXtensible Host Controller
Driver,system32\DRIVERS\iusb3xhc.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,kbdclass,Keyboard Class
Driver,system32\DRIVERS\kbdclass.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,KSecDD,,System32\Drivers\ksecdd.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,KSecPkg,,System32\Drivers\ksecpkg.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,lltdio,Link-Layer Topology Discovery Mapper I/O
Driver,system32\DRIVERS\lltdio.sys,Kernel driver,Auto Start,
Wed Apr 20 15:40:45
2016Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drive
rs\luafv.sys,File system driver,Auto Start,
Wed Apr 20 15:40:45 2016Z,MEIx64,Intel(R) Management Engine Interface
,system32\DRIVERS\TeeDriverx64.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,mfenlfk,McAfee NDIS Light
Filter,system32\DRIVERS\mfenlfk.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,mfewfpk,McAfee Inc.
mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,mouclass,Mouse Class
Driver,system32\DRIVERS\mouclass.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mou
ntmgr.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45
2016Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,System32\drivers\mpsdrv.s
ys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mr
xdav.sys,File system driver,Manual,
Wed Apr 20 15:40:45
2016Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,Fil
e system driver,Manual,
Wed Apr 20 15:40:45
2016Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys
,File system driver,Manual,
Wed Apr 20 15:40:45
2016Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys
,File system driver,Manual,
Wed Apr 20 15:40:45 2016Z,Msfs,,,File system driver,System Start,
Wed Apr 20 15:40:45 2016Z,msisadrv,,system32\drivers\msisadrv.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45
2016Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,File
system driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,NativeWifiP,NativeWiFi
Filter,system32\DRIVERS\nwifi.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Ke
Page 157

SYSTEM OUTPUT.txt
rnel driver,Boot Start,
Wed Apr 20 15:40:45
2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sy
s,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,Ndisuio,NDIS Usermode I/O
Protocol,system32\DRIVERS\ndisuio.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,
Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,NDProxy,NDIS Proxy,,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,NetBIOS,NetBIOS
Interface,system32\DRIVERS\netbios.sys,File system driver,System Start,
Wed Apr 20 15:40:45
2016Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,K
ernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,NETwNs64,___ Intel(R) Wireless Adapter Driver for Windows
7 - 64 Bit,system32\DRIVERS\Netwsw02.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,Npfs,,,File system driver,System Start,
Wed Apr 20 15:40:45
2016Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsipr
oxy.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,Ntfs,,,File system driver,Manual,
Wed Apr 20 15:40:45 2016Z,Null,,,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,nvpciflt,,system32\DRIVERS\nvpciflt.sys,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45 2016Z,O2FJ2RDR,,system32\DRIVERS\O2FJ2w7x64.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45
2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partm
gr.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,pci,PCI Bus Driver,system32\drivers\pci.sys,Kernel
driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel
driver,Auto Start,
Wed Apr 20 15:40:45
2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp
.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,prepdrvr,SMS Process Event
Driver,system32\DRIVERS\prepdrv.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,prot_2k,,,Kernel driver,Boot Start,
Wed Apr 20 15:40:45
2016Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sy
s,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,RasAgileVpn,WAN Miniport
(IKEv2),system32\DRIVERS\AgileVpn.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,
Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\raspppoe.sy
s,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,K
ernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File
system driver,System Start,
Wed Apr 20 15:40:45 2016Z,rdpbus,Remote Desktop Device Redirector Bus
Driver,system32\DRIVERS\rdpbus.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,System32\DRIVERS\RDPCDD.

Page 158

SYSTEM OUTPUT.txt

sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,RDPDR,Terminal Server Device Redirector
Driver,System32\drivers\rdpdr.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,RDPENCDD,@%systemroot%\system32\drivers\RDPENCDD.sys;-101,system32\drivers\rdp
encdd.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45
2016Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdp
refmp.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,RDPWD,RDP Winstation Driver,,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,rspndr,Link-Layer Topology Discovery
Responder,system32\DRIVERS\rspndr.sys,Kernel driver,Auto Start,
Wed Apr 20 15:40:45 2016Z,Serenum,Serenum Filter
Driver,system32\DRIVERS\serenum.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,Serial,Serial port
driver,system32\DRIVERS\serial.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,spldr,Security Processor Loader Driver,,Kernel driver,Boot
Start,
Wed Apr 20 15:40:45
2016Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,File
system driver,Manual,
Wed Apr 20 15:40:45
2016Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,File
system driver,Manual,
Wed Apr 20 15:40:45 2016Z,srvnet,,System32\DRIVERS\srvnet.sys,File system
driver,Manual,
Wed Apr 20 15:40:45 2016Z,stdcfltn,Disk Class Filter Driver for
Accelerometer,system32\DRIVERS\stdcfltn.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,swenum,Software Bus
Driver,system32\DRIVERS\swenum.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Ke
rnel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,
Wed Apr 20 15:40:45 2016Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45
2016Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,system32\DRIVERS\tdx.sys,Kernel
driver,System Start,
Wed Apr 20 15:40:45 2016Z,TermDD,Terminal Device
Driver,system32\DRIVERS\termdd.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45
2016Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,System32\DRIVERS\tss
ecsrv.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,tunnel,Microsoft Tunnel Miniport Adapter
Driver,system32\DRIVERS\tunnel.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,umbus,UMBus Enumerator
Driver,system32\DRIVERS\umbus.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,usbehci,Microsoft USB 2.0 Enhanced Host Controller
Miniport Driver,system32\DRIVERS\usbehci.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,vdrvroot,Microsoft Virtual Drive Enumerator
Driver,system32\drivers\vdrvroot.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,VgaSave,,\SystemRoot\System32\drivers\vga.sys,Kernel
driver,System Start,
Wed Apr 20 15:40:45 2016Z,volmgr,Volume Manager
Driver,system32\drivers\volmgr.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45
2016Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmg
rx.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,volsnap,Storage
volumes,system32\drivers\volsnap.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,vpnva,Cisco AnyConnect Secure Mobility Client Virtual

Page 159

SYSTEM OUTPUT.txt
Miniport Adapter for Windows x64,system32\DRIVERS\vpnva64-6.sys,Kernel
driver,Manual,
Wed Apr 20 15:40:45 2016Z,vwifibus,Virtual WiFi Bus
Driver,system32\DRIVERS\vwifibus.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,vwififlt,Virtual WiFi Filter
Driver,system32\DRIVERS\vwififlt.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45
2016Z,wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,system32\DRIVERS\wanarp.sys,
Kernel driver,System Start,
Wed Apr 20 15:40:45
2016Z,wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wd
f01000.sys,Kernel driver,Boot Start,
Wed Apr 20 15:40:45 2016Z,WfpLwf,WFP Lightweight
Filter,system32\DRIVERS\wfplwf.sys,Kernel driver,System Start,
Wed Apr 20 15:40:45 2016Z,WmiAcpi,Microsoft Windows Management Interface for
ACPI,system32\DRIVERS\wmiacpi.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45
2016Z,WudfPf,@%SystemRoot%\system32\drivers\Wudfpf.sys;-1000,system32\drivers\WudfPf
.sys,Kernel driver,Manual,
Wed Apr 20 15:40:45 2016Z,WUDFRd,Windows Driver Foundation - User-mode Driver
Framework Reflector,system32\DRIVERS\WUDFRd.sys,Kernel driver,Manual,
Wed Apr 20 15:39:52 2016Z,drmkaud,Microsoft Trusted Audio
Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel driver,Manual,
Wed Apr 20 13:19:57 2016Z,macmnsvc,McAfee Agent Common Services,"C:\Program Files
(x86)\McAfee\Common Framework\macmnsvc.exe" /ServiceStart,Own_Process,Auto Start,NT
AUTHORITY\LocalService
Wed Apr 20 13:19:57 2016Z,masvc,McAfee Agent Service,"C:\Program Files
(x86)\McAfee\Common Framework\masvc.exe" /ServiceStart,Own_Process,Auto
Start,LocalSystem
Wed Apr 20 13:19:57 2016Z,McAfeeFramework,McAfee Agent Backwards Compatibility
Service,"C:\Program Files (x86)\McAfee\Common
Framework\x86\macompatsvc.exe",Own_Process,Manual,LocalSystem
Wed Apr 20 13:19:43 2016Z,mfefire,McAfee Firewall Core Service,"C:\Program
Files\Common Files\McAfee\SystemCore\\mfefire.exe",Own_Process,Manual,LocalSystem
Wed Apr 20 13:19:40 2016Z,McShield,McAfee McShield,"C:\Program Files\Common
Files\McAfee\SystemCore\\mcshield.exe",Own_Process,Auto Start,LocalSystem
Wed Apr 20 13:19:38 2016Z,mfevtp,McAfee Validation Trust Protection
Service,"C:\WINDOWS\system32\mfevtps.exe",Own_Process,Auto Start,LocalSystem
Wed Apr 20 13:19:10 2016Z,enterceptAgent,McAfee Host Intrusion Prevention
Service,"C:\Program Files\McAfee\Host Intrusion
Prevention\FireSvc.exe",Own_Process,Auto Start,LocalSystem
Tue Apr 19 20:40:52 2016Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program
Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe",Own_Process,Manual,LocalSystem
Tue Apr 19 20:40:07 2016Z,gupdate,Google Update Service (gupdate),"C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe" /svc,Own_Process,Auto Start,LocalSystem
Tue Apr 19 20:40:07 2016Z,gupdatem,Google Update Service (gupdatem),"C:\Program
Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,Own_Process,Manual,LocalSystem
Tue Apr 19 20:03:56
2016Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,Own_Process,Manual,NT
AUTHORITY\NetworkService
Tue Apr 19 20:00:35 2016Z,CmRcService,Configuration Manager Remote
Control,C:\WINDOWS\CCM\RemCtrl\CmRcService.exe,Own_Process,Auto Start,LocalSystem
Tue Apr 19 20:00:19 2016Z,CcmFramework,,,,,,
Tue Apr 19 19:48:22 2016Z,USBSTOR,USB Mass Storage
Driver,system32\DRIVERS\USBSTOR.SYS,Kernel driver,Manual,
Tue Apr 19 19:47:44
2016Z,EapHost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem
Mon Apr 18 16:26:07 2016Z,MSKSSRV,Microsoft Streaming Service
Proxy,system32\drivers\MSKSSRV.sys,Kernel driver,Manual,
Mon Apr 18 16:17:34 2016Z,ipsec,,,,,
Mon Apr 18 16:17:34 2016Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Page 160

SYSTEM OUTPUT.txt
Mon Apr 18 16:17:30 2016Z,Browser,Computer Browser,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Disabled,LocalSystem
Mon Apr 18 16:17:30 2016Z,HomeGroupListener,HomeGroup
Listener,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Disabled,LocalSystem
Mon Apr 18 16:17:30 2016Z,HomeGroupProvider,HomeGroup
Provider,%SystemRoot%\System32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Disabled,NT AUTHORITY\LocalService
Mon Apr 18 16:17:30 2016Z,WPCSvc,Parental Controls,%SystemRoot%\system32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Disabled,NT Authority\LocalService
Mon Apr 18 16:03:47 2016Z,HipShieldK,McAfee Inc.
HipShieldK,system32\drivers\HipShieldK.sys,Kernel driver,Manual,
Mon Apr 18 16:02:36 2016Z,HipMgmt,McAfee Host Intrusion Prevention lpc
Service,"C:\Program Files (x86)\McAfee\Host Intrusion
Prevention\HipMgmt.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 16:02:15 2016Z,FireNfcp,McAfee Inc.
FireNfcp,system32\drivers\FireNfcp.sys,Kernel driver,Manual,
Mon Apr 18 15:58:37 2016Z,McTaskManager,McAfee Task Manager,"C:\Program Files
(x86)\McAfee\VirusScan Enterprise\VsTskMgr.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:58:26 2016Z,SNMP,,,,,
Mon Apr 18 15:57:48 2016Z,PCP,,,,,
Mon Apr 18 15:57:46
2016Z,eventlog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost
.exe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Mon Apr 18 15:57:46
2016Z,Pointsec,Pointsec,C:\WINDOWS\SysWOW64\Prot_srv.exe,272,Auto Start,LocalSystem
Mon Apr 18 15:57:46 2016Z,Pointsec_Start,Pointsec Service
Start,C:\WINDOWS\SysWOW64\PstartSr.exe,272,Auto Start,LocalSystem
Mon Apr 18 15:57:14 2016Z,CVPND,Cisco Systems; Inc. VPN Service,"C:\Program Files
(x86)\Cisco Systems\VPN Client\cvpnd.exe",272,Auto Start,LocalSystem
Mon Apr 18 15:57:04 2016Z,{2A088A0C-A99B-4B11-81C8-178260EEB892},,,,,
Mon Apr 18 15:56:59 2016Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,
Mon Apr 18 15:56:53 2016Z,{915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3},,,,,
Mon Apr 18 15:56:52 2016Z,vpnagent,Cisco AnyConnect Secure Mobility
Agent,"C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\vpnagent.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:54:46 2016Z,atashost,WebEx Service Host for Support
Center,"C:\WINDOWS\SysWOW64\atashost.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:54:18
2016Z,enstart64,enstart64,C:\WINDOWS\system32\enstart64.exe,Own_Process,Auto
Start,LocalSystem
Mon Apr 18 15:50:45
2016Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%Syst
emRoot%\system32\IEEtwCollector.exe /V,Own_Process,Manual,LocalSystem
Mon Apr 18 15:50:45 2016Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,,
Mon Apr 18 15:48:25 2016Z,MSDTC Bridge 4.0.0.0,,,,,
Mon Apr 18 15:48:25 2016Z,SMSvcHost 4.0.0.0,,,,,
Mon Apr 18 15:48:25 2016Z,Windows Workflow Foundation 4.0.0.0,,,,,
Mon Apr 18 15:45:34 2016Z,ac.sharedstore,ActivIdentity Shared Store
Service,"C:\Program Files\Common
Files\ActivIdentity\ac.sharedstore.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:45:16 2016Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,
Mon Apr 18 15:45:08 2016Z,AdobeFlashPlayerUpdateSvc,Adobe Flash Player Update
Service,C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe,Own_Process,
Manual,LocalSystem
Mon Apr 18 15:44:49 2016Z,AdobeARMservice,Adobe Acrobat Update Service,"C:\Program
Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe",Own_Process,Auto
Start,LocalSystem
Mon Apr 18 15:43:23 2016Z,ASP.NET_4.0.30319,,,,,
Mon Apr 18 15:43:21 2016Z,ASP.NET,,,,,
Mon Apr 18 15:43:18 2016Z,aspnet_state,ASP.NET State
Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe,Own_Proce
Page 161

SYSTEM OUTPUT.txt
ss,Manual,NT AUTHORITY\NetworkService
Mon Apr 18 15:43:15 2016Z,.NET Memory Cache 4.0,,,,,
Mon Apr 18 15:43:15
2016Z,NetMsmqActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll;-8195,"C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"
-NetMsmqActivator,Share_Process,Disabled,NT AUTHORITY\NetworkService
Mon Apr 18 15:43:15
2016Z,NetPipeActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll;-8197,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,S
hare_Process,Disabled,NT AUTHORITY\LocalService
Mon Apr 18 15:43:15
2016Z,NetTcpActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModel
InstallRC.dll;-8199,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,Sh
are_Process,Disabled,NT AUTHORITY\LocalService
Mon Apr 18 15:43:15
2016Z,NetTcpPortSharing,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMod
elInstallRC.dll;-8201,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,
Share_Process,Disabled,NT AUTHORITY\LocalService
Mon Apr 18 15:42:19 2016Z,clr_optimization_v4.0.30319_32,Microsoft .NET Framework
NGEN
v4.0.30319_X86,C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,Own_Proces
s,Auto Start,LocalSystem
Mon Apr 18 15:42:19 2016Z,clr_optimization_v4.0.30319_64,Microsoft .NET Framework
NGEN
v4.0.30319_X64,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,Own_Proc
ess,Auto Start,LocalSystem
Mon Apr 18 15:42:14 2016Z,.NET CLR Networking 4.0.0.0,,,,,
Mon Apr 18 15:42:12 2016Z,clr_optimization_v2.0.50727_32,Microsoft .NET Framework
NGEN
v2.0.50727_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,Own_Proc
ess,Disabled,LocalSystem
Mon Apr 18 15:42:12 2016Z,clr_optimization_v2.0.50727_64,Microsoft .NET Framework
NGEN
v2.0.50727_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,Own_Pr
ocess,Disabled,LocalSystem
Mon Apr 18 15:37:48 2016Z,dcdbas,System Management
Driver,system32\DRIVERS\dcdbas64.sys,Kernel driver,Manual,
Mon Apr 18 15:34:47 2016Z,BthEnum,Bluetooth Enumerator
Service,system32\DRIVERS\BthEnum.sys,Kernel driver,Manual,
Mon Apr 18 15:34:47 2016Z,BthPan,Bluetooth Device (Personal Area
Network),system32\DRIVERS\bthpan.sys,Kernel driver,Manual,
Mon Apr 18 15:34:47 2016Z,RFCOMM,Bluetooth Device (RFCOMM Protocol
TDI),system32\DRIVERS\rfcomm.sys,Kernel driver,Manual,
Mon Apr 18 15:34:46 2016Z,BTHUSB,Bluetooth Radio USB
Driver,System32\Drivers\BTHUSB.sys,Kernel driver,Manual,
Mon Apr 18 15:31:22 2016Z,CcmExec,SMS Agent
Host,C:\WINDOWS\CCM\CcmExec.exe,Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:31:22 2016Z,smstsmgr,ConfigMgr Task Sequence
Agent,C:\WINDOWS\CCM\TSManager.exe /service,Own_Process,Manual,LocalSystem
Mon Apr 18 15:30:46 2016Z,lpasvc,Microsoft Policy Platform Local
Authority,"C:\Program Files\Microsoft Policy Platform\policyHost.exe"
/service,Share_Process,Manual,LocalSystem
Mon Apr 18 15:30:46 2016Z,lppsvc,Microsoft Policy Platform Processor,"C:\Program
Files\Microsoft Policy Platform\policyHost.exe"
/service,Share_Process,Manual,LocalSystem
Mon Apr 18 15:30:13
2016Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.
exe,Share_Process,Auto Start,LocalSystem
Mon Apr 18 15:30:12 2016Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own_Process,Manual,LocalSystem
Mon Apr 18 15:30:12
2016Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.ex
e -k netsvcs,Share_Process,Auto Start,LocalSystem
Page 162

\

SYSTEM OUTPUT.txt

```
Mon Apr 18 15:29:32
2016Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Mon Apr 18 15:29:32 2016Z,Wlansvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,
Mon Apr 18 15:29:03 2016Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Mon Apr 18 15:29:01 2016Z,WinDefend,@%ProgramFiles%\Windows
Defender\MsMpRes.dll;-103,%SystemRoot%\System32\svchost.exe -k
secsvcs,Share_Process,Manual,LocalSystem\
Mon Apr 18 15:28:58 2016Z,{4525A64F-379A-4D68-8A81-DA5AA833E191},,,,,
Mon Apr 18 15:28:54
2016Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Mon Apr 18 15:28:54
2016Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Mon Apr 18 15:28:51 2016Z,BTHPORT,Bluetooth Port
Driver,System32\Drivers\BTHport.sys,Kernel driver,Manual,
Mon Apr 18 15:28:13 2016Z,MSPQM,Microsoft Streaming Quality Manager
Proxy,system32\drivers\MSPQM.sys,Kernel driver,Manual,
Mon Apr 18 15:28:13 2016Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink
Converter,system32\drivers\MSTEE.sys,Kernel driver,Manual,
Mon Apr 18 15:28:12 2016Z,MSPCLOCK,Microsoft Streaming Clock
Proxy,system32\drivers\MSPCLOCK.sys,Kernel driver,Manual,
Mon Apr 18 15:28:07 2016Z,RtkAudioService,Realtek Audio Service,"C:\Program
Files\Realtek\Audio\HDA\RtkAudioService64.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:28:04
2016Z,Wlansvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Mon Apr 18 15:28:03 2016Z,{033026B9-7329-415D-8068-DD988B393525},,,,,
Mon Apr 18 15:28:02
2016Z,O2FLASH,O2FLASH,%SystemRoot%\system32\DRIVERS\o2flash.exe,Own_Process,Auto
Start,LocalSystem
Mon Apr 18 15:28:01 2016Z,nvsvc,NVIDIA Display Driver
Service,"C:\WINDOWS\system32\nvvsvc.exe",Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:27:42 2016Z,ApHidMonitorService,Alps HID Monitor Service,C:\Program
Files\DellTPad\HidMonitorSvc.exe,Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:27:40 2016Z,{4BA4B36E-29B2-45EB-8693-07A52C8F3CC5},,,,,
Mon Apr 18 15:27:22 2016Z,ialm,,,,,
Mon Apr 18 15:27:21 2016Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
Service,%SystemRoot%\system32\igfxCUIService.exe,Own_Process,Auto Start,LocalSystem
Mon Apr 18 15:26:58 2016Z,atapi,,\SystemRoot\system32\drivers\atapi.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,cdrom,,\SystemRoot\system32\drivers\cdrom.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,HpSAMD,,\SystemRoot\system32\drivers\HpSAMD.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,LSI_SAS,,\SystemRoot\system32\drivers\lsi_sas.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,LSI_SCSI,,\SystemRoot\system32\drivers\lsi_scsi.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,MegaSR,,\SystemRoot\system32\drivers\MegaSR.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,msahci,,\SystemRoot\system32\drivers\msahci.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,Kernel
driver,Manual,
Mon Apr 18 15:26:58 2016Z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,Kernel
driver,Manual,
```

Page 163

SYSTEM OUTPUT.txt
Mon Apr 18 15:26:58 2016Z,Wd,,\SystemRoot\system32\drivers\wd.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,aliide,,\SystemRoot\system32\drivers\aliide.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,arc,,\SystemRoot\system32\drivers\arc.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,LSI_FC,,\SystemRoot\system32\drivers\lsi_fc.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,LSI_SAS2,,\SystemRoot\system32\drivers\lsi_sas2.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,ST7007,,\SystemRoot\system32\drivers\ST7007.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,Kernel driver,Manual,
Mon Apr 18 15:26:57 2016Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,Kernel driver,Manual,
Mon Apr 18 15:26:55 2016Z,TsUsbGD,Remote Desktop Generic USB

Page 164

SYSTEM OUTPUT.txt
Device,\SystemRoot\system32\drivers\TsUsbGD.sys,Kernel driver,Manual,
Mon Apr 18 15:24:49 2016Z,bcmnfcusb,NFC USB Bus
Driver,\SystemRoot\system32\drivers\bcmnfcusb7.sys,Kernel driver,Manual,
Mon Apr 18 15:23:49 2016Z,ISCT,Intel(R) Smart Connect Technology Device
Driver,\SystemRoot\system32\drivers\ISCTD.sys,Kernel driver,Manual,
Mon Apr 18 15:22:46 2016Z,iwsehub,Intel(R) WSE Hub
Driver,\SystemRoot\system32\drivers\iwsehub.sys,Kernel driver,Manual,
Mon Apr 18 15:22:46 2016Z,iwsepal,Intel(R) WSE-PAL
Driver,\SystemRoot\system32\drivers\iwsepal.sys,Kernel driver,Manual,
Mon Apr 18 15:22:43 2016Z,swmbbnmea05,Sierra Wireless USB Device for NMEA Serial
Communication - Dell,\SystemRoot\system32\drivers\swmbbnmea05.sys,Kernel
driver,Manual,
Mon Apr 18 15:22:43 2016Z,swmbbser05,Sierra Wireless USB Device for Serial
Communication - Dell,\SystemRoot\system32\drivers\swmbbser05.sys,Kernel
driver,Manual,
Mon Apr 18 15:22:42 2016Z,swg3knmea05,Sierra Wireless QMI NMEA Communication -
Dell,\SystemRoot\system32\drivers\swg3knmea05.sys,Kernel driver,Manual,
Mon Apr 18 15:22:42 2016Z,swg3kser05,Sierra Wireless QMI USB Device for Legacy
Serial Communication - Dell,\SystemRoot\system32\drivers\swg3kser05.sys,Kernel
driver,Manual,
Mon Apr 18 15:22:42 2016Z,swibus05,Sierra Wireless Bus Enumerator
05,\SystemRoot\system32\drivers\swibus05.sys,Kernel driver,Manual,
Mon Apr 18 15:22:42 2016Z,swibusflt05,Sierra Wireless Bus Enumerator Filter
05,\SystemRoot\system32\drivers\swibusflt05.sys,Kernel driver,Manual,
Mon Apr 18 15:22:42 2016Z,swimbbbus05,Sierra Wireless MBB Device Bus Enumerator
05,\SystemRoot\system32\drivers\swimbbbus05.sys,Kernel driver,Manual,
Mon Apr 18 15:22:42 2016Z,swimbbbusflt05,Sierra Wireless MBB Device Bus Enumerator
Filter 05,\SystemRoot\system32\drivers\swimbbbusflt05.sys,Kernel driver,Manual,
Wed Dec 30 14:09:15 2015Z,VMBusHID,,\SystemRoot\system32\drivers\VMBusHID.sys,Kernel
driver,Manual,
Wed Dec 30 14:08:57 2015Z,tsusbhub,Remote Deskotop USB
Hub,\SystemRoot\system32\drivers\tsusbhub.sys,Kernel driver,Manual,
Wed Dec 30 14:08:56 2015Z,fdc,Floppy Disk Controller
Driver,\SystemRoot\system32\drivers\fdc.sys,Kernel driver,Manual,
Wed Dec 30 14:08:48 2015Z,flpydisk,Floppy Disk
Driver,\SystemRoot\system32\drivers\flpydisk.sys,Kernel driver,Manual,
Wed Dec 30 14:08:47 2015Z,Synth3dVsc,Microsoft Virtual 3D Video Transport
Driver,\SystemRoot\system32\drivers\Synth3dVsc.sys,Kernel driver,Manual,
Wed Dec 30 14:08:18 2015Z,s3cap,,\SystemRoot\system32\drivers\vms3cap.sys,Kernel
driver,Manual,
Wed Dec 30 14:05:27
2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\Se
archIndexer.exe /Embedding,Own_Process,Auto Start,LocalSystem
Wed Dec 30 14:05:22
2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Wed Dec 30 13:52:01 2015Z,netvsc,,system32\DRIVERS\netvsc60.sys,Kernel
driver,Manual,
Wed Dec 30 13:52:01 2015Z,SynthVid,,system32\DRIVERS\VMBusVideoM.sys,Kernel
driver,Manual,
Wed Dec 30 13:52:00 2015Z,secdrv,Security Driver,,Kernel driver,Disabled,
Wed Dec 30 13:52:00 2015Z,udfs,udfs,system32\DRIVERS\udfs.sys,File system
driver,Disabled,
Wed Dec 30 12:33:10
2015Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Auto Start,LocalSystem
Wed Dec 30 12:27:20
2015Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
regsvc,Share_Process,Auto Start,NT AUTHORITY\LocalService
Wed Dec 30 12:27:10
2015Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k bthsvcs,Share_Process,Disabled,NT AUTHORITY\LocalService
Page 165

SYSTEM OUTPUT.txt

Wed Dec 30 12:26:59
2015Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k netsvcs,Share_Process,Disabled,LocalSystem
Wed Dec 30 10:09:44 2015Z,amdxata,,system32\drivers\amdxata.sys,Kernel driver,Boot
Start,
Wed Dec 30 09:12:34
2015Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k WbioSvcGroup,Share_Process,Manual,LocalSystem
Wed Dec 30 07:48:59 2015Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k
GPSvcGroup,Own_Process,Auto Start,LocalSystem
Wed Dec 30 07:41:07
2015Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\
svchost.exe -k utcsvc,Own_Process,Auto Start,LocalSystem
Wed Dec 30 07:41:07
2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,
Wed Dec 30 07:41:07
2015Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho
st.exe -k LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService
Wed Dec 30 07:41:07
2015Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,
Wed Dec 30 07:41:07 2015Z,iScsiPrt,iScsiPort
Driver,\SystemRoot\system32\drivers\msiscsi.sys,Kernel driver,Manual,
Wed Dec 30 07:41:07 2015Z,terminpt,Microsoft Remote Desktop Input
Driver,\SystemRoot\system32\drivers\terminpt.sys,Kernel driver,Manual,
Wed Dec 30 07:41:07 2015Z,usbcir,eHome Infrared Receiver
(USBCIR),\SystemRoot\system32\drivers\usbcir.sys,Kernel driver,Manual,
Wed Dec 30 07:41:07
2015Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wa
t\WatAdminSvc.exe,Own_Process,Manual,LocalSystem
Wed Dec 30 07:41:07
2015Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Wed Dec 30 07:41:07
2015Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Wed Dec 30 07:03:57 2015Z,MSDTC Bridge 3.0.0.0,,,,,
Wed Dec 30 07:03:57 2015Z,ServiceModelEndpoint 3.0.0.0,,,,,
Wed Dec 30 07:03:57 2015Z,ServiceModelOperation 3.0.0.0,,,,,
Wed Dec 30 07:03:57 2015Z,ServiceModelService 3.0.0.0,,,,,
Wed Dec 30 07:03:57 2015Z,SMSvcHost 3.0.0.0,,,,,
Wed Dec 30 07:03:57 2015Z,Windows Workflow Foundation 3.0.0.0,,,,,
Tue Dec 29 15:55:14 2015Z,Microsoft SharePoint Workspace Audit Service,Microsoft
SharePoint Workspace Audit Service,"C:\Program Files (x86)\Microsoft
Office\Office14\GROOVE.EXE" /auditservice,Own_Process,Manual,NT
AUTHORITY\LocalService
Tue Dec 29 15:55:13 2015Z,Outlook,,,,,
Tue Dec 29 15:55:12 2015Z,adsi,,,,,
Tue Dec 29 15:52:10 2015Z,osppsvc,Office Software Protection Platform,"C:\Program
Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",Own_Process,Manual,NT
AUTHORITY\NetworkService
Tue Dec 29 15:51:22
2015Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost
.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Dec 29 15:51:11 2015Z,ose,Office  Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",Own_Process,Manual,LocalSystem
Tue Apr 12 07:45:41
2011Z,CscService,@%systemroot%\system32\cscsvc.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Apr 12 07:45:24
2011Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem
Tue Apr 12 07:45:24

Page 166

SYSTEM OUTPUT.txt
2011Z,peerdistsvc,@%SystemRoot%\system32\peerdistsvc.dll:-9000,%SystemRoot%\system32
\svchost.exe -k PeerDist,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Apr 12 07:45:24 2011Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,\SystemRoot\system32\drivers\rdpvideominiport.sys,Kernel driver,Manual,
Tue Apr 12 07:45:24 2011Z,sensrsvc,@%SystemRoot%\system32\sensrsvc.dll:-1000,%SystemRoot%\system32\svcho
st.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Tue Apr 12 07:45:24 2011Z,storsvc,@%SystemRoot%\system32\storsvc.dll:-100,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Apr 12 07:45:24 2011Z,umrdpservice,@%SystemRoot%\system32\umrdp.dll:-1000,%SystemRoot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Apr 12 07:45:24 2011Z,VGPU,,SystemRoot\system32\drivers\rdvgkmd.sys,Kernel driver,Manual
Tue Apr 12 07:45:22 2011Z,AppMgmt,Parameters,,%SystemRoot%\System32\appmgmts.dll,,,
Tue Apr 12 07:45:22 2011Z,CscService,Parameters,,%SystemRoot%\System32\cscsvc.dll,,,
Tue Apr 12 07:45:22
2011Z,peerdistsvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,
Tue Apr 12 07:45:22 2011Z,RDPUDD,,,,
Tue Apr 12 07:45:22 2011Z,sensrsvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,
Tue Apr 12 07:45:22 2011Z,storsvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,
Tue Apr 12 07:45:22
2011Z,umrdpservice\Parameters,,%SystemRoot%\system32\umrdp.dll,,,
Tue Apr 12 07:44:54 2011Z,dmvsc,,\SystemRoot\system32\drivers\dmvsc.sys,Kernel
driver,Manual,
Sun Nov 21 03:58:24 2010Z,BTHMODEM,Bluetooth Serial Communications
driver,\SystemRoot\system32\drivers\bthmodem.sys,Kernel driver,Manual,
Sun Nov 21 03:58:22 2010Z,gagp30kx,Microsoft Generic AGPV3.0 Filter for K8 Processor
Platforms,\SystemRoot\system32\drivers\gagp30kx.sys,Kernel driver,Manual,
Sun Nov 21 03:58:22 2010Z,uagp35,Microsoft AGPV3.5
Filter,\SystemRoot\system32\drivers\uagp35.sys,Kernel driver,Manual,
Sun Nov 21 03:58:21 2010Z,b06bdrv,Broadcom NetXtreme II
VBD,\SystemRoot\system32\drivers\bxvbda.sys,Kernel driver,Manual,
Sun Nov 21 03:58:21 2010Z,HidBth,Microsoft Bluetooth HID
Miniport,\SystemRoot\system32\drivers\hidbth.sys,Kernel driver,Manual,
Sun Nov 21 03:58:19 2010Z,amdk8,AMD K8 Processor
Driver,\SystemRoot\system32\drivers\amdk8.sys,Kernel driver,Manual,
Sun Nov 21 03:58:19 2010Z,amdppm,AMD Processor
Driver,\SystemRoot\system32\drivers\amdppm.sys,Kernel driver,Manual,
Sun Nov 21 03:58:19 2010Z,processor,Processor
Driver,\SystemRoot\system32\drivers\processor.sys,Kernel driver,Manual,
Sun Nov 21 03:58:18 2010Z,ebdrv,Broadcom NetXtreme II 10 GigE
VBD,\SystemRoot\system32\drivers\evbda.sys,Kernel driver,Manual,
Sun Nov 21 03:58:17 2010Z,pcmcia,,\SystemRoot\system32\drivers\pcmcia.sys,Kernel
driver,Manual,
Sun Nov 21 03:58:16 2010Z,MTConfig,Microsoft Input Configuration
Driver,\SystemRoot\system32\drivers\MTConfig.sys,Kernel driver,Manual,
Sun Nov 21 03:58:15 2010Z,circlass,Consumer IR
Devices,\SystemRoot\system32\drivers\circlass.sys,Kernel driver,Manual,
Sun Nov 21 03:58:13 2010Z,sffloppy,High-Capacity Floppy Disk
Drive,\SystemRoot\system32\drivers\sffloppy.sys,Kernel driver,Manual,
Sun Nov 21 03:58:11 2010Z,HidBatt,HID UPS Battery
Driver,\SystemRoot\system32\drivers\HidBatt.sys,Kernel driver,Manual,
Sun Nov 21 03:58:08 2010Z,HidIr,Microsoft Infrared HID
Driver,\SystemRoot\system32\drivers\hidir.sys,Kernel driver,Manual,
Sun Nov 21 03:58:07 2010Z,sermouse,Serial Mouse
Driver,\SystemRoot\system32\drivers\sermouse.sys,Kernel driver,Manual,
Sun Nov 21 03:58:06 2010Z,BrFiltLo,Brother USB Mass-Storage Lower Filter
Driver,\SystemRoot\system32\drivers\BrFiltLo.sys,Kernel driver,Manual,
Sun Nov 21 03:58:06 2010Z,BrFiltUp,Brother USB Mass-Storage Upper Filter
Driver,\SystemRoot\system32\drivers\BrFiltUp.sys,Kernel driver,Manual,
Sun Nov 21 03:58:05 2010Z,usbohci,Microsoft USB Open Host Controller Miniport

SYSTEM_OUTPUT.txt

```
Driver,\SystemRoot\system32\drivers\usbohci.sys,Kernel driver,Manual,
Sun Nov 21 03:58:05 2010Z,usbuhci,Microsoft USB Universal Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbuhci.sys,Kernel driver,Manual,
Sun Nov 21 03:58:00 2010Z,Wacompen,Wacom Serial Pen HID
Driver,\SystemRoot\system32\drivers\wacompen.sys,Kernel driver,Manual,
Sun Nov 21 03:57:59 2010Z,crcdisk,Crcdisk Filter
Driver,\SystemRoot\system32\drivers\crcdisk.sys,Kernel driver,Manual,
Sun Nov 21 03:57:58 2010Z,UmPass,Microsoft UMPass
Driver,\SystemRoot\system32\drivers\umpass.sys,Kernel driver,Disabled,
Sun Nov 21 03:57:56 2010Z,usbprint,Microsoft USB PRINTER
Class,\SystemRoot\system32\drivers\usbprint.sys,Kernel driver,Manual,
Sun Nov 21 03:46:56 2010Z,b57nd60a,Broadcom NetXtreme Gigabit Ethernet - NDIS
6.0,system32\DRIVERS\b57nd60a.sys,Kernel driver,Manual,
Sun Nov 21 03:46:56 2010Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,CD/DVD File System
driver,Manual,
Sun Nov 21 03:46:56 2010Z,fastfat,FAT12/16/32 File System
Driver,\SystemRoot\system32\drivers\fastfat,FAT12/16/32 File System Driver,,File system driver,Disabled,
Sun Nov 21 03:39:53 2010Z,Dhcp,Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,
Sun Nov 21 03:46:56 2010Z,vga,,system32\DRIVERS\vgapnp.sys,Kernel driver,Manual,
Sun Nov 21 03:38:46 2010Z,TsusbF1t,,system32\drivers\tsusbflt.sys,Kernel
driver,Manual,
Sun Nov 21 03:33:56
2010Z,SessionEnv,@%SystemRoot%\System32\SessEnv.d11;-1026,%SystemRoot%\System32\svch
ost.exe -k netsvcs,Share_Process,Manual,localSystem
Sun Nov 21 03:29:32 2010Z,1394ohci,1394 OHCI Compliant Host
Controller,\SystemRoot\system32\drivers\1394ohci.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,AcpiPmi,ACPI Power Meter
Driver,\SystemRoot\system32\drivers\acpipmi.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,agp440,Intel AGP Bus
Filter,\SystemRoot\system32\drivers\agp440.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,ErrDev,Microsoft Hardware Error Device
Driver,\SystemRoot\system32\drivers\errdev.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,IPMIDRV,,\SystemRoot\system32\drivers\IPMIDrv.sys,Kernel
driver,Manual,
Sun Nov 21 03:29:32 2010Z,nv_agp,NVIDIA nForce AGP Bus
Filter,\SystemRoot\system32\drivers\nv_agp.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,ohci1394,OHCI Compliant Host Controller
(Legacy),\SystemRoot\system32\drivers\ohci1394.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,sffdisk,SFF Storage Class
Driver,\SystemRoot\system32\drivers\sffdisk.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_mmc,SFF Storage Protocol Driver for
MMC,\SystemRoot\system32\drivers\sffp_mmc.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_sd,SFF Storage Protocol Driver for
SDBus,\SystemRoot\system32\drivers\sffp_sd.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,u1iagpkx,Uli AGP Bus
Filter,\SystemRoot\system32\drivers\uliagpkx.sys,Kernel driver,Manual,
Sun Nov 21 03:29:32 2010Z,vhdmp,,\SystemRoot\system32\drivers\vhdmp.sys,Kernel
driver,Manual,
Tue Jul 14 05:34:12 2009Z,BDESVC,Parameters,,%SystemRoot%\System32\bdesvc.dll,,,
Tue Jul 14 05:34:12
2009Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,
Tue Jul 14 05:34:12 2009Z,wPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2pimsvc\Parameters,,%SystemRoot%\System32\pnrpsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2psvc\Parameters,,%SystemRoot%\System32\p2psvc.dll,,,
Tue Jul 14 05:34:09 2009Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,
Tue Jul 14 05:08:55 2009Z,iph1psvc\Parameters,,%SystemRoot%\System32\iph1psvc.dll,,,
Tue Jul 14 04:54:38 2009Z,NdisCap,NDIS Capture Lightweight
Filter,\system32\DRIVERS\ndiscap.sys,Kernel driver,Manual,
Tue Jul 14 04:54:32 2009Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,
Tue Jul 14 04:54:31 2009Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,
Tue Jul 14 04:54:25
2009Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,
Tue Jul 14 04:54:05 2009Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,
```

SYSTEM OUTPUT.txt

```
Tue Jul 14 04:53:57
2009Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,Kernel
driver,Manual,
Tue Jul 14 04:53:56 2009Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Tue Jul 14 04:53:48 2009Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcss.dll,,,
Tue Jul 14 04:53:45
2009Z,TrkWks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:53:45 2009Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Tue Jul 14 04:53:36
2009Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:53:36
2009Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Tue Jul 14 04:53:33
2009Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32
\svchost.exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Tue Jul 14 04:53:25 2009Z,WmiApRpl,,,,,
Tue Jul 14 04:53:24
2009Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,localSystem
Tue Jul 14 04:53:24
2009Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,Own_Process,Manual,localSystem
Tue Jul 14 04:53:21 2009Z,TCPIP6,Microsoft IPv6 Protocol
Driver,system32\DRIVERS\tcpip.sys,Kernel driver,Manual,
Tue Jul 14 04:53:21
2009Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,Ke
rnel driver,Manual,
Tue Jul 14 04:53:20
2009Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Jul 14 04:53:19
2009Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService
Tue Jul 14 04:53:19 2009Z,Winsock,,,Adapter,Manual,
Tue Jul 14 04:49:48
2009Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Sha
re_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:48
2009Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:46
2009Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:45
2009Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,Share_Process,Disabled,localSystem
Tue Jul 14 04:49:45
2009Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Tue Jul 14 04:49:35
2009Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:35 2009Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Tue Jul 14 04:49:35
2009Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
```

Page 169

SYSTEM OUTPUT.txt
```
xe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:26 2009Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Tue Jul 14 04:49:24
2009Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT AUTHORITY\LocalService
Tue Jul 14 04:49:24 2009Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:24
2009Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:24 2009Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:23 2009Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Tue Jul 14 04:49:22 2009Z,TBS\Parameters,,%SystemRoot%\System32\tbssvc.dll,,,
Tue Jul 14 04:49:20 2009Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Tue Jul 14 04:49:18 2009Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Tue Jul 14 04:49:08 2009Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Data,,,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Networking,,,,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for Oracle,,,,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for SqlServer,,,,,
Tue Jul 14 04:49:01 2009Z,.NETFramework,,,,,
Tue Jul 14 04:49:01
2009Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svcho
st.exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own_Proc
ess,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\ap
pid.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
Authority\LocalService
Tue Jul 14 04:49:01 2009Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\System32\svchost.
exe -k netsvcs,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\Sys
tem32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Tue Jul 14 04:49:01
2009Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,, --
Tue Jul 14 04:49:01
2009Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchos
t.exe -k AxInstSVGroup,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,
Tue Jul 14 04:49:01 2009Z,BattC,,,,,
Tue Jul 14 04:49:01
```
Page 170

SYSTEM OUTPUT.txt

2009Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,
Tue Jul 14 04:49:01 2009Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,
Tue Jul 14 04:49:01 2009Z,Brserid,Brother MFC Serial Port Interface Driver
(WDM),\SystemRoot\System32\Drivers\Brserid.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,BrSerWdm,Brother WDM Serial
driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbMdm,Brother MFC USB Fax Only
Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbSer,Brother MFC USB Serial WDM
Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,
Tue Jul 14 04:49:01
2009Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,crypt32,,,,,
Tue Jul 14 04:49:01
2009Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k NetworkService,Share_Process,Auto Start,NT Authority\NetworkService
Tue Jul 14 04:49:01 2009Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,DCLocator,,,,,
Tue Jul 14 04:49:01
2009Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svch
ost.exe -k defragsvc,Own_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,
Tue Jul 14 04:49:01
2009Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Sha
re_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,ESENT,,,,,
Tue Jul 14 04:49:01
2009Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,
Tue Jul 14 04:49:01 2009Z,exfat,exFAT File System Driver,,File system driver,Manual,
Tue Jul 14 04:49:01
2009Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,
Tue Jul 14 04:49:01 2009Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,
Tue Jul 14 04:49:01
2009Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,File system driver,Manual,
Tue Jul 14 04:49:01
2009Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot
%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own_Process,Manual,NT
Authority\LocalService
Tue Jul 14 04:49:01
2009Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers
\FsDepends.sys,File system driver,Manual,
Tue Jul 14 04:49:01 2009Z,hcw85cir,Hauppauge Consumer Infrared
Receiver,\SystemRoot\system32\drivers\hcw85cir.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Page 171

SYSTEM OUTPUT.txt
Tue Jul 14 04:49:01 2009Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,
Tue Jul 14 04:49:01
2009Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows
Communication
Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v
3.0\Windows Communication Foundation\infocard.exe",Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,
Tue Jul 14 04:49:01 2009Z,inetaccs,,,,,
Tue Jul 14 04:49:01
2009Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt
drv.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchos
t.exe -k NetSvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.
sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share_Process,Manual,L
ocalSystem
Tue Jul 14 04:49:01 2009Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,
Tue Jul 14 04:49:01 2009Z,ldap,,,,,
Tue Jul 14 04:49:01
2009Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.ex
e.-k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,Lsa,,,,,
Tue Jul 14 04:49:01
2009Z,MMCSS,@%systemroot%\system32\mmcss.dll;-100,%SystemRoot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,MMCSS\Parameters,,%SystemRoot%\system32\mmcss.dll,,,
Tue Jul 14 04:49:01 2009Z,Modem,,system32\drivers\modem.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svc
host.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,
Tue Jul 14 04:49:01
2009Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System
32\drivers\mshidkmdf.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchos
t.exe -k netsvcs,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,
Tue Jul 14 04:49:01
2009Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.
exe /V,Own_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,MsRPC,,,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,MSSCNTRS,,,,,
Page 172

SYSTEM OUTPUT.txt

Tue Jul 14 04:49:01
2009Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.
exe -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,
Tue Jul 14 04:49:01
2009Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchos
t.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,netprofm\Parameters,,%SystemRoot%\System32\netprofm.dll,,,
Tue Jul 14 04:49:01
2009Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,Share_Process,Auto Start,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,NTDS,,,,,
Tue Jul 14 04:49:01
2009Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PerfDisk,,,,,
Tue Jul 14 04:49:01
2009Z,PerfHost,@%systemroot%\syswow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PerfNet,,,,,
Tue Jul 14 04:49:01 2009Z,PerfOS,,,,,
Tue Jul 14 04:49:01 2009Z,PerfProc,,,,,
Tue Jul 14 04:49:01
2009Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,
Tue Jul 14 04:49:01
2009Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchos
t.exe -k DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\sv
chost.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost
.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\sv
chost.exe -k NetworkServiceNetworkRestricted,Share_Process,Manual,NT
Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PortProxy,,,,,
Tue Jul 14 04:49:01
2009Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,
Tue Jul 14 04:49:01
2009Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Page 173

SYSTEM OUTPUT.txt

Tue Jul 14 04:49:01 2009Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,ProtectedStorage,@%systemroot%\system32\psbase.dll;-300,%SystemRoot%\system32\
lsass.exe,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,
Tue Jul 14 04:49:01
2009Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\d
rivers\qwavedrv.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,RDPDD,,,,,
Tue Jul 14 04:49:01 2009Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,,
Tue Jul 14 04:49:01
2009Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator
.exe,Own_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,RpcSs,@oleres.dll;-5010,%SystemRoot%\system32\svchost.exe
-k rpcss,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,
Tue Jul 14 04:49:01
2009Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.ex
e -k SDRSVC,Own_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.e
xe -k netsvcs,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,
Tue Jul 14 04:49:01
2009Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,
Tue Jul 14 04:49:01
2009Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,
Tue Jul 14 04:49:01
2009Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Disabled,LocalSystem
Tue Jul 14 04:49:01
2009Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,
Tue Jul 14 04:49:01
2009Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System3
2\svchost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Tue Jul 14 04:49:01
2009Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap
.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.ex
e,272,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe
Page 174

SYSTEM OUTPUT.txt
,Own_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,sppuinotify,@%SystemRoot%\system32\sppuinotify.dll;-103,%SystemRoot%\system32\
svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,sppuinotify\Parameters,,%SystemRoot%\system32\sppuinotify.dll,,,
Tue Jul 14 04:49:01
2009Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,          \
Tue Jul 14 04:49:01
2009Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT Authority\LocalService
Tue Jul 14 04:49:01
2009Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.ex
e -k imgsvc,Own_Process,Manual,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Tue Jul 14 04:49:01
2009Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe
-k swprv,Own_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Tue Jul 14 04:49:01
2009Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Tue Jul 14 04:49:01
2009Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchos
t.exe -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Tue Jul 14 04:49:01
2009Z,TBS,@%SystemRoot%\system32\tbssvc.dll;-100,%SystemRoot%\System32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TCPIP6TUNNEL,,,,,
Tue Jul 14 04:49:01 2009Z,TCPIPTUNNEL,,,,,
Tue Jul 14 04:49:01 2009Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,Kernel
driver,Manual,
Tue Jul 14 04:49:01
2009Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,Share_Process,Manual,NT Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
host.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Tue Jul 14 04:49:01
2009Z,THREADORDER,@%systemroot%\system32\mmcss.dll;-102,%SystemRoot%\system32\svchos
t.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TSDDD,,,,,
Tue Jul 14 04:49:01 2009Z,UGatherer,,,,,
Tue Jul 14 04:49:01 2009Z,UGTHRSVC,,,,,
Tue Jul 14 04:49:01
2009Z,UIODetect,@%SystemRoot%\system32\uiOdetect.exe;-101,%SystemRoot%\system32\UIOD
etect.exe,272,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Tue Jul 14 04:49:01

Page 175

SYSTEM OUTPUT.txt
2009Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,localSystem
Tue Jul 14 04:49:01 2009Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,
Tue Jul 14 04:49:01
2009Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Proc
ess,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_
Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,W3SVC,,,,,
Tue Jul 14 04:49:01
2009Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",Own_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,WbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcssvc,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Tue Jul 14 04:49:01
2009Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Tue Jul 14 04:49:01
2009Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,File
system driver,Manual,
Tue Jul 14 04:49:01 2009Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WinSock2,,,,,
Tue Jul 14 04:49:01 2009Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe",Own_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\
drivers\ws2ifsl.sys,Kernel driver,Disabled,
Tue Jul 14 04:49:01
2009Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
Page 176

SYSTEM OUTPUT.txt
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WSearchIdxPi,,,,,,
Tue Jul 14 04:49:01 2009Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Tue Jul 14 04:49:01 2009Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalServiceNoNetwork,Share_Process,Manual,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,
Tue Jul 14 04:49:01 2009Z,xmlprov,,,,,
Tue Jul 14 02:34:41 2009Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Tue Jul 14 02:34:41 2009Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
------------------------------------------
svc_plus v.20120625
(System) Lists services/drivers in Services key by LastWrite times in a short format
with warnings for type mismatches
^^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.

ControlSet001\Services
Lists services/drivers in Services key by LastWrite times in a short format with
warnings for type mismatches
^^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.

Thu Apr 28 15:00:49 2016Z,mferkdet,McAfee Inc.
mferkdet,system32\drivers\mferkdet.sys,,Manual,
Thu Apr 28 15:00:38 2016Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,,Manual,
Thu Apr 28 15:00:36 2016Z,mfeapfk,McAfee Inc.
mfeapfk,system32\drivers\mfeapfk.sys,,Manual,
Wed Apr 20 15:58:48
2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot
%\servicing\TrustedInstaller.exe,,Manual,****localSystem
Wed Apr 20 15:42:05 2016Z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,,Boot Start,
Wed Apr 20 15:42:04 2016Z,DisplayLinkService,DisplayLinkManager,"C:\Program
Files\DisplayLink Core Software\DisplayLinkManager.exe",^^^^272,2,LocalSystem
Wed Apr 20 15:41:02
2016Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asyncmac.sy
s,,Manual,
Wed Apr 20 15:40:59
2016Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,
Wed Apr 20 15:40:59 2016Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,,Manual,
Wed Apr 20 15:40:59 2016Z,mfeavfk01,McAfee Inc.,,,Manual,
Wed Apr 20 15:40:59 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common
Files\McAfee\SystemCore\\mfemms.exe",,Auto Start,****LocalSystem
Wed Apr 20 15:40:59 2016Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Wed Apr 20 15:40:59
2016Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,
Wed Apr 20 15:40:52 2016Z,cvusbdrv,Dell
ControlVault,System32\Drivers\cvusbdrv.sys,,Manual,
Wed Apr 20 15:40:52 2016Z,kbdhid,Keyboard HID
Driver,system32\DRIVERS\kbdhid.sys,,Manual,
Wed Apr 20 15:40:52 2016Z,mouhid,Mouse HID
Page 177

SYSTEM OUTPUT.txt
Driver,system32\DRIVERS\mouhid.sys,,Manual,
Wed Apr 20 15:40:52
2016Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfi
lter.sys,,Manual,
Wed Apr 20 15:40:52 2016Z,WinUsb,WinUSB Driver,system32\DRIVERS\WinUSB.sys,,Manual,
Wed Apr 20 15:40:51 2016Z,HidUsb,Microsoft HID Class
Driver,system32\DRIVERS\hidusb.sys,,Manual,
Wed Apr 20 15:40:51 2016Z,monitor,Microsoft Monitor Class Function Driver
Service,system32\DRIVERS\monitor.sys,,Manual,
Wed Apr 20 15:40:51 2016Z,usbccgp,Microsoft USB Generic Parent
Driver,system32\DRIVERS\usbccgp.sys,,Manual,
Wed Apr 20 15:40:51 2016Z,usbvideo,USB Video Device
(WDM),System32\Drivers\usbvideo.sys,,Manual,
Wed Apr 20 15:40:50 2016Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,,Manual,
Wed Apr 20 15:40:49 2016Z,IntcAzAudAddService,Service for Realtek HD Audio
(WDM),system32\drivers\RTDVHD64.sys,,Manual,
Wed Apr 20 15:40:49 2016Z,iusb3hub,Intel(R) USB 3.0 Hub
Driver,system32\DRIVERS\iusb3hub.sys,,Manual,
Wed Apr 20 15:40:49 2016Z,ST_Accel,STMicroelectronics Accelerometer
Service,system32\DRIVERS\ST_Accel.sys,,Manual,
Wed Apr 20 15:40:48 2016Z,IntcDAud,Intel(R) Display
Audio,system32\DRIVERS\IntcDAud.sys,,Manual,
Wed Apr 20 15:40:48 2016Z,ksthunk,Kernel Streaming
Thunks,\SystemRoot\system32\drivers\ksthunk.sys,,Manual,
Wed Apr 20 15:40:48 2016Z,Parport,Parallel port
driver,system32\DRIVERS\parport.sys,,Manual,
Wed Apr 20 15:40:48 2016Z,usbhub,Microsoft USB Standard Hub
Driver,system32\DRIVERS\usbhub.sys,,Manual,
Wed Apr 20 15:40:47 2016Z,mssmbios,Microsoft System Management BIOS
Driver,system32\DRIVERS\mssmbios.sys,,System Start,
Wed Apr 20 15:40:46 2016Z,nvlddmkm,,system32\DRIVERS\nvlddmkm.sys,,Manual,
Wed Apr 20 15:40:46 2016Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,,Boot
Start,
Wed Apr 20 15:40:45 2016Z,ACPI,Microsoft ACPI Driver,system32\drivers\ACPI.sys,,Boot
Start,
Wed Apr 20 15:40:45 2016Z,acsock,acsock,system32\DRIVERS\acsock64.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\
afd.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,ApfiltrService,Alps Touch Pad Filter Driver for Windows
x64,system32\DRIVERS\Apfiltr.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,Beep,Beep,,,System Start,
Wed Apr 20 15:40:45 2016Z,blbdrive,,system32\DRIVERS\blbdrive.sys,,System Start,
Wed Apr 20 15:40:45
2016Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,,Ma
nual,
Wed Apr 20 15:40:45 2016Z,CipcCdp,Cisco IP Communicator driver for
CDP,system32\DRIVERS\CipcCdp.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45
2016Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,System32\CLFS.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,CmBatt,Microsoft ACPI Control Method Battery
Driver,system32\DRIVERS\CmBatt.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,CNG,,System32\Drivers\cng.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,Compbatt,Microsoft Composite Battery
Driver,system32\DRIVERS\compbatt.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,CompositeBus,Composite Bus Enumerator
Driver,system32\DRIVERS\CompositeBus.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,CSC,@%systemroot%\system32\cscsvc.dll;-202,system32\drivers\csc.sys,,System
Start,
Wed Apr 20 15:40:45 2016Z,ctxusbm,Citrix USB Monitor
Driver,system32\DRIVERS\ctxusbm.sys,,System Start,
Page 178

SYSTEM OUTPUT.txt
Wed Apr 20 15:40:45 2016Z,CVirtA,Cisco Systems VPN Adapter for 64-bit
Windows,system32\DRIVERS\CVirtA64.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,CVPNDRVA,Cisco Systems Inc. IPSec
Driver,\??\C:\WINDOWS\system32\Drivers\CVPNDRVA.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,DfsC,@%systemroot%\system32\drivers\dfsc.sys;-101,System32\Drivers\dfsc.sys,,S
ystem Start,
Wed Apr 20 15:40:45
2016Z,discache,@%systemroot%\system32\drivers\discache.sys;-102,System32\drivers\dis
cache.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,Disk,Disk Driver,system32\drivers\disk.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,DNE,Deterministic Network Enhancer
Miniport,system32\DRIVERS\dne64x.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,dptf_acpi,,system32\DRIVERS\dptf_acpi.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,dptf_cpu,,system32\DRIVERS\dptf_cpu.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,e1dexpress,Intel(R) PRO/1000 PCI Express Network
Connection Driver D,system32\DRIVERS\e1d62x64.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,enstart64_,enstart64_,\??\C:\WINDOWS\system32\enstart64_.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,esif_lf,,system32\DRIVERS\esif_lf.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,system32\drivers\fil
einfo.sys,,Boot Start,
Wed Apr 20 15:40:45
2016Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmg
r.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,Fs_Rec,,,^^^^8,0,
Wed Apr 20 15:40:45
2016Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.
sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,HDAudBus,Microsoft UAA Bus Driver for High Definition
Audio,system32\DRIVERS\HDAudBus.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,,Man
ual,
Wed Apr 20 15:40:45
2016Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwp
olicy.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,i8042prt,i8042 Keyboard and PS/2 Mouse Port
Driver,system32\DRIVERS\i8042prt.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,iaStorA,,system32\drivers\iaStorA.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,iaStorF,,system32\drivers\iaStorF.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,igfx,,system32\DRIVERS\igdkmd64.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,intelppm,Intel Processor
Driver,system32\DRIVERS\intelppm.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,iusb3xhc,Intel(R) USB 3.0 eXtensible Host Controller
Driver,system32\DRIVERS\iusb3xhc.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,kbdclass,Keyboard Class
Driver,system32\DRIVERS\kbdclass.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,KSecDD,,System32\Drivers\ksecdd.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,KSecPkg,,System32\Drivers\ksecpkg.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,lltdio,Link-Layer Topology Discovery Mapper I/O
Driver,system32\DRIVERS\lltdio.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45
2016Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drive
rs\luafv.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45 2016Z,MEIx64,Intel(R) Management Engine Interface
,system32\DRIVERS\TeeDriverx64.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,mfenlfk,McAfee NDIS Light
Filter,system32\DRIVERS\mfenlfk.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,mfewfpk,McAfee Inc.
Page 179

SYSTEM OUTPUT.txt
mfewfpk,system32\drivers\mfewfpk.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,mouclass,Mouse Class
Driver,system32\DRIVERS\mouclass.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mou
ntmgr.sys,,Boot Start,
Wed Apr 20 15:40:45
2016Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,System32\drivers\mpsdrv.s
ys,,Manual,
Wed Apr 20 15:40:45
2016Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mr
xdav.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,,Ma
nual,
Wed Apr 20 15:40:45
2016Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys
,,Manual,
Wed Apr 20 15:40:45
2016Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys
,,Manual,
Wed Apr 20 15:40:45 2016Z,Msfs,,,,System Start,
Wed Apr 20 15:40:45 2016Z,msisadrv,,system32\drivers\msisadrv.sys,,Boot Start,
Wed Apr 20 15:40:45
2016Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,,Boot
Start,
Wed Apr 20 15:40:45 2016Z,NativeWifiP,NativeWiFi
Filter,system32\DRIVERS\nwifi.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,,B
oot Start,
Wed Apr 20 15:40:45
2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sy
s,,Manual,
Wed Apr 20 15:40:45 2016Z,Ndisuio,NDIS Usermode I/O
Protocol,system32\DRIVERS\ndisuio.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,
,Manual,
Wed Apr 20 15:40:45 2016Z,NDProxy,NDIS Proxy,,,Manual,
Wed Apr 20 15:40:45 2016Z,NetBIOS,NetBIOS
Interface,system32\DRIVERS\netbios.sys,,System Start,
Wed Apr 20 15:40:45
2016Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,,
System Start,
Wed Apr 20 15:40:45 2016Z,NETwNs64,___ Intel(R) Wireless Adapter Driver for Windows
7 - 64 Bit,system32\DRIVERS\Netwsw02.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,Npfs,,,,System Start,
Wed Apr 20 15:40:45
2016Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsipr
oxy.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,Ntfs,,,,Manual,
Wed Apr 20 15:40:45 2016Z,Null,,,,System Start,
Wed Apr 20 15:40:45 2016Z,nvpciflt,,system32\DRIVERS\nvpciflt.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,O2FJ2RDR,,system32\DRIVERS\O2FJ2w7x64.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partm
gr.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,pci,PCI Bus Driver,system32\drivers\pci.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,PEAUTH,PEAUTH,scem32\drivers\peauth.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45

Page 180

SYSTEM OUTPUT.txt
2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp
.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,prepdrvr,SMS Process Event
Driver,system32\DRIVERS\prepdrv.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,prot_2k,,,,Boot Start,
Wed Apr 20 15:40:45
2016Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sy
s,,System Start,
Wed Apr 20 15:40:45 2016Z,RasAgileVpn,WAN Miniport
(IKEv2),system32\DRIVERS\AgileVpn.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,
,Manual,
Wed Apr 20 15:40:45
2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\raspppoe.sy
s,,Manual,
Wed Apr 20 15:40:45
2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,,
Manual,
Wed Apr 20 15:40:45
2016Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,,Syst
em Start,
Wed Apr 20 15:40:45 2016Z,rdpbus,Remote Desktop Device Redirector Bus
Driver,system32\DRIVERS\rdpbus.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,System32\DRIVERS\RDPCDD.
sys,,System Start,
Wed Apr 20 15:40:45 2016Z,RDPDR,Terminal Server Device Redirector
Driver,System32\drivers\rdpdr.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,RDPENCDD,@%systemroot%\system32\drivers\RDPENCDD.sys;-101,system32\drivers\rdp
encdd.sys,,System Start,
Wed Apr 20 15:40:45
2016Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdp
refmp.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,RDPWD,RDP Winstation Driver,,,Manual,
Wed Apr 20 15:40:45 2016Z,rspndr,Link-Layer Topology Discovery
Responder,system32\DRIVERS\rspndr.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45 2016Z,Serenum,Serenum Filter
Driver,system32\DRIVERS\serenum.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,Serial,Serial port
driver,system32\DRIVERS\serial.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,spldr,Security Processor Loader Driver,,,Boot Start,
Wed Apr 20 15:40:45
2016Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,srvnet,,System32\DRIVERS\srvnet.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,stdcfltn,Disk Class Filter Driver for
Accelerometer,system32\DRIVERS\stdcfltn.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,swenum,Software Bus
Driver,system32\DRIVERS\swenum.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,,B
oot Start,
Wed Apr 20 15:40:45 2016Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,,<<<<Auto Start,
Wed Apr 20 15:40:45 2016Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,,Manual,
Wed Apr 20 15:40:45
2016Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,system32\DRIVERS\tdx.sys,,Syste
m Start,
Wed Apr 20 15:40:45 2016Z,TermDD,Terminal Device
Driver,system32\DRIVERS\termdd.sys,,System Start,
Page 181

SYSTEM OUTPUT.txt

Wed Apr 20 15:40:45 2016Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,System32\DRIVERS\tssecsrv.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,tunnel,Microsoft Tunnel Miniport Adapter Driver,system32\DRIVERS\tunnel.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,umbus,UMBus Enumerator Driver,system32\DRIVERS\umbus.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,usbehci,Microsoft USB 2.0 Enhanced Host Controller Miniport Driver,system32\DRIVERS\usbehci.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,vdrvroot,Microsoft Virtual Drive Enumerator Driver,system32\drivers\vdrvroot.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,VgaSave,,\SystemRoot\System32\drivers\vga.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,volmgr,Volume Manager Driver,system32\drivers\volmgr.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmgrx.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,volsnap,Storage volumes,system32\drivers\volsnap.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,vpnva,Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows x64,system32\DRIVERS\vpnva64-6.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,vwifibus,Virtual WiFi Bus Driver,system32\DRIVERS\vwifibus.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,vwififlt,Virtual WiFi Filter Driver,system32\DRIVERS\vwififlt.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,Wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,system32\DRIVERS\wanarp.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wdf01000.sys,,Boot Start,
Wed Apr 20 15:40:45 2016Z,WfpLwf,WFP Lightweight Filter,system32\DRIVERS\wfplwf.sys,,System Start,
Wed Apr 20 15:40:45 2016Z,WmiAcpi,Microsoft Windows Management Interface for ACPI,system32\DRIVERS\wmiacpi.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,WudfPf,@%SystemRoot%\system32\drivers\Wudfpf.sys;-1000,system32\drivers\WudfPf.sys,,Manual,
Wed Apr 20 15:40:45 2016Z,WUDFRd,Windows Driver Foundation - User-mode Driver Framework Reflector,system32\DRIVERS\WUDFRd.sys,,Manual,
Wed Apr 20 15:39:52 2016Z,drmkaud,Microsoft Trusted Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,,Manual,
Wed Apr 20 13:19:57 2016Z,macmnsvc,McAfee Agent Common Services,"C:\Program Files (x86)\McAfee\Common Framework\macmnsvc.exe" /ServiceStart,,Auto Start,****NT AUTHORITY\LocalService
Wed Apr 20 13:19:57 2016Z,masvc,McAfee Agent Service,"C:\Program Files (x86)\McAfee\Common Framework\masvc.exe" /ServiceStart,,Auto Start,****LocalSystem
Wed Apr 20 13:19:57 2016Z,McAfeeFramework,McAfee Agent Backwards Compatibility Service,"C:\Program Files (x86)\McAfee\Common Framework\x86\macompatsvc.exe",,Manual,****LocalSystem
Wed Apr 20 13:19:43 2016Z,mfefire,McAfee Firewall Core Service,"C:\Program Files\Common Files\McAfee\SystemCore\\mfefire.exe",,Manual,****LocalSystem
Wed Apr 20 13:19:40 2016Z,McShield,McAfee McShield,"C:\Program Files\Common Files\McAfee\SystemCore\\mcshield.exe",,Auto Start,****LocalSystem
Wed Apr 20 13:19:38 2016Z,mfevtp,McAfee Validation Trust Protection Service,"C:\WINDOWS\system32\mfevtps.exe",,Auto Start,****LocalSystem
Wed Apr 20 13:19:10 2016Z,enterceptAgent,McAfee Host Intrusion Prevention Service,"C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe",,Auto Start,****LocalSystem
Tue Apr 19 20:40:52 2016Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe",,Manual,****LocalSystem

Page 182

SYSTEM OUTPUT.txt
Tue Apr 19 20:40:07 2016Z,gupdate,Google Update Service (gupdate),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc,,Auto Start,****LocalSystem
Tue Apr 19 20:40:07 2016Z,gupdatem,Google Update Service (gupdatem),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,,Manual,****LocalSystem
Tue Apr 19 20:03:56 2016Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,,Manual,****NT AUTHORITY\NetworkService
Tue Apr 19 20:00:35 2016Z,CmRcService,Configuration Manager Remote Control,C:\WINDOWS\CCM\RemCtrl\CmRcService.exe,,Auto Start,****LocalSystem
Tue Apr 19 20:00:19 2016Z,CcmFramework,,,^^^^,,
Tue Apr 19 19:48:22 2016Z,USBSTOR,USB Mass Storage Driver,system32\DRIVERS\USBSTOR.SYS,,Manual,
Tue Apr 19 19:47:44 2016Z,EapHost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe -k netsvcs,,Manual,****localSystem
Mon Apr 18 16:26:07 2016Z,MSKSSRV,Microsoft Streaming Service Proxy,system32\drivers\MSKSSRV.sys,,Manual,
Mon Apr 18 16:17:34 2016Z,ipsec,,,^^^^,,
Mon Apr 18 16:17:34 2016Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Mon Apr 18 16:17:30 2016Z,Browser,Computer Browser,%SystemRoot%\System32\svchost.exe -k netsvcs,,Disabled,****LocalSystem
Mon Apr 18 16:17:30 2016Z,HomeGroupListener,HomeGroup Listener,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,,Disabled,****LocalSystem
Mon Apr 18 16:17:30 2016Z,HomeGroupProvider,HomeGroup Provider,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Disabled,****NT AUTHORITY\LocalService
Mon Apr 18 16:17:30 2016Z,WPCSvc,Parental Controls,%SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted,,Disabled,****NT Authority\LocalService
Mon Apr 18 16:03:47 2016Z,HipShieldK,McAfee Inc. HipShieldK,system32\drivers\HipShieldK.sys,,Manual,
Mon Apr 18 16:02:36 2016Z,HipMgmt,McAfee Host Intrusion Prevention lpc Service,"C:\Program Files (x86)\McAfee\Host Intrusion Prevention\HipMgmt.exe",,Auto Start,****LocalSystem
Mon Apr 18 16:02:15 2016Z,FireNfcp,McAfee Inc. FireNfcp,system32\drivers\FireNfcp.sys,,Manual,
Mon Apr 18 15:58:37 2016Z,McTaskManager,McAfee Task Manager,"C:\Program Files (x86)\McAfee\VirusScan Enterprise\VsTskMgr.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:58:26 2016Z,SNMP,,,^^^^,,
Mon Apr 18 15:57:48 2016Z,PCP,,,^^^^,,
Mon Apr 18 15:57:46 2016Z,eventlog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Mon Apr 18 15:57:46 2016Z,Pointsec,Pointsec,C:\WINDOWS\SysWOW64\Prot_srv.exe,^^^^272,2,LocalSystem
Mon Apr 18 15:57:46 2016Z,Pointsec_Start,Pointsec Service Start,C:\WINDOWS\SysWOW64\PstartSr.exe,^^^^272,2,LocalSystem
Mon Apr 18 15:57:14 2016Z,CVPND,Cisco Systems, Inc. VPN Service,"C:\Program Files (x86)\Cisco Systems\VPN Client\cvpnd.exe",^^^^272,2,LocalSystem
Mon Apr 18 15:57:04 2016Z,{2A088A0C-A99B-4B11-81C8-178260EEB892},,,^^^^,,
Mon Apr 18 15:56:59 2016Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,
Mon Apr 18 15:56:53 2016Z,{915C51E9-6775-4D3C-8C2C-2FBB7DE5D3C3},,,^^^^,,
Mon Apr 18 15:56:52 2016Z,vpnagent,Cisco AnyConnect Secure Mobility Agent,"C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:54:46 2016Z,atashost,WebEx Service Host for Support Center,"C:\WINDOWS\SysWOW64\atashost.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:54:18 2016Z,enstart64,enstart64,C:\WINDOWS\system32\enstart64.exe,,Auto Start,****LocalSystem
Mon Apr 18 15:50:45 2016Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%SystemRoot%\system32\IEEtwCollector.exe /V,,Manual,****LocalSystem
Page 183

SYSTEM OUTPUT.txt
Mon Apr 18 15:50:45 2016Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,,
Mon Apr 18 15:48:25 2016Z,MSDTC Bridge 4.0.0.0,,,^^^^,,
Mon Apr 18 15:48:25 2016Z,SMSvcHost 4.0.0.0,,,^^^^,,
Mon Apr 18 15:48:25 2016Z,Windows Workflow Foundation 4.0.0.0,,,^^^^,,
Mon Apr 18 15:45:34 2016Z,ac.sharedstore,ActivIdentity Shared Store
Service,"C:\Program Files\Common Files\ActivIdentity\ac.sharedstore.exe",,Auto
Start,****LocalSystem
Mon Apr 18 15:45:16 2016Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,
Mon Apr 18 15:45:08 2016Z,AdobeFlashPlayerUpdateSvc,Adobe Flash Player Update
Service,C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe,,Manual,****
LocalSystem
Mon Apr 18 15:44:49 2016Z,AdobeARMservice,Adobe Acrobat Update Service,"C:\Program
Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:43:23 2016Z,ASP.NET_4.0.30319,,,^^^^,,
Mon Apr 18 15:43:21 2016Z,ASP.NET,,,^^^^,,
Mon Apr 18 15:43:18 2016Z,aspnet_state,ASP.NET State
Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe,,Manual,*
***NT AUTHORITY\NetworkService
Mon Apr 18 15:43:15 2016Z,.NET Memory Cache 4.0,,,^^^^,,
Mon Apr 18 15:43:15
2016Z,NetMsmqActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll;-8195,"C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"
-NetMsmqActivator,,Disabled,****NT AUTHORITY\NetworkService
Mon Apr 18 15:43:15
2016Z,NetPipeActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode
lInstallRC.dll;-8197,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,,
Disabled,****NT AUTHORITY\LocalService
Mon Apr 18 15:43:15
2016Z,NetTcpActivator,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceModel
InstallRC.dll;-8199,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,,D
isabled,****NT AUTHORITY\LocalService
Mon Apr 18 15:43:15
2016Z,NetTcpPortSharing,@C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\\ServiceMod
elInstallRC.dll;-8201,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,
,Disabled,****NT AUTHORITY\LocalService
Mon Apr 18 15:42:19 2016Z,clr_optimization_v4.0.30319_32,Microsoft .NET Framework
NGEN v4.0.30319_X86,C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,,Auto
Start,****LocalSystem
Mon Apr 18 15:42:19 2016Z,clr_optimization_v4.0.30319_64,Microsoft .NET Framework
NGEN
v4.0.30319_X64,C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,,Auto
Start,****LocalSystem
Mon Apr 18 15:42:14 2016Z,.NET CLR Networking 4.0.0.0,,,^^^^,,
Mon Apr 18 15:42:12 2016Z,clr_optimization_v2.0.50727_32,Microsoft .NET Framework
NGEN
v2.0.50727_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,,Disable
d,****LocalSystem
Mon Apr 18 15:42:12 2016Z,clr_optimization_v2.0.50727_64,Microsoft .NET Framework
NGEN
v2.0.50727_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,,Disab
led,****LocalSystem
Mon Apr 18 15:37:48 2016Z,dcdbas,System Management
Driver,system32\DRIVERS\dcdbas64.sys,,Manual,
Mon Apr 18 15:34:47 2016Z,BthEnum,Bluetooth Enumerator
Service,system32\DRIVERS\BthEnum.sys,,Manual,
Mon Apr 18 15:34:47 2016Z,BthPan,Bluetooth Device (Personal Area
Network),system32\DRIVERS\bthpan.sys,,Manual,
Mon Apr 18 15:34:47 2016Z,RFCOMM,Bluetooth Device (RFCOMM Protocol
TDI),system32\DRIVERS\rfcomm.sys,,Manual,
Mon Apr 18 15:34:46 2016Z,BTHUSB,Bluetooth Radio USB
Driver,System32\Drivers\BTHUSB.sys,,Manual,
Mon Apr 18 15:31:22 2016Z,CcmExec,SMS Agent Host,C:\WINDOWS\CCM\CcmExec.exe,,Auto
Start,****LocalSystem

Page 184

SYSTEM OUTPUT.txt

Mon Apr 18 15:31:22 2016Z,smstsmgr,ConfigMgr Task Sequence
Agent,C:\WINDOWS\CCM\TSManager.exe /service,,Manual,****LocalSystem
Mon Apr 18 15:30:46 2016Z,lpasvc,Microsoft Policy Platform Local
Authority,"C:\Program Files\Microsoft Policy Platform\policyHost.exe"
/service,,Manual,****LocalSystem
Mon Apr 18 15:30:46 2016Z,lppsvc,Microsoft Policy Platform Processor,"C:\Program
Files\Microsoft Policy Platform\policyHost.exe" /service,,Manual,****LocalSystem
Mon Apr 18 15:30:13
2016Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.
exe,,Auto Start,****LocalSystem
Mon Apr 18 15:30:12 2016Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,,Manual,****LocalSystem
Mon Apr 18 15:30:12
2016Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.ex
e -k netsvcs,,Auto Start,****LocalSystem
Mon Apr 18 15:29:32
2016Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Mon Apr 18 15:29:32 2016Z,Wlansvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,
Mon Apr 18 15:29:03 2016Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Mon Apr 18 15:29:01 2016Z,WinDefend,@%ProgramFiles%\Windows
Defender\MsMpRes.dll;-103,%SystemRoot%\System32\svchost.exe -k
secsvcs,,Manual,****LocalSystem
Mon Apr 18 15:28:58 2016Z,{4525A64F-379A-4D68-8A81-DA5AA833E191},,,^^^^,,
Mon Apr 18 15:28:54
2016Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****LocalSystem
Mon Apr 18 15:28:54
2016Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,,Auto Start,****NT AUTHORITY\LocalService
Mon Apr 18 15:28:51 2016Z,BTHPORT,Bluetooth Port
Driver,System32\Drivers\BTHport.sys,,Manual,
Mon Apr 18 15:28:13 2016Z,MSPQM,Microsoft Streaming Quality Manager
Proxy,system32\drivers\MSPQM.sys,,Manual,
Mon Apr 18 15:28:13 2016Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink
Converter,system32\drivers\MSTEE.sys,,Manual,
Mon Apr 18 15:28:12 2016Z,MSPCLOCK,Microsoft Streaming Clock
Proxy,system32\drivers\MSPCLOCK.sys,,Manual,
Mon Apr 18 15:28:07 2016Z,RtkAudioService,Realtek Audio Service,"C:\Program
Files\Realtek\Audio\HDA\RtkAudioService64.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:28:04
2016Z,Wlansvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Mon Apr 18 15:28:03 2016Z,{033026B9-7329-415D-8068-DD988B393525},,,^^^^,,
Mon Apr 18 15:28:02
2016Z,O2FLASH,O2FLASH,%SystemRoot%\system32\DRIVERS\o2flash.exe,,Auto
Start,****LocalSystem
Mon Apr 18 15:28:01 2016Z,nvsvc,NVIDIA Display Driver
Service,"C:\WINDOWS\system32\nvvsvc.exe",,Auto Start,****LocalSystem
Mon Apr 18 15:27:42 2016Z,ApHidMonitorService,Alps HID Monitor Service,C:\Program
Files\DellTPad\HidMonitorSvc.exe,,Auto Start,****LocalSystem
Mon Apr 18 15:27:40 2016Z,{4BA4B36E-29B2-45EB-8693-07A52C8F3CC5},,,^^^^,,
Mon Apr 18 15:27:22 2016Z,ialm,,,^^^^,,
Mon Apr 18 15:27:21 2016Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
Service,%SystemRoot%\system32\igfxCUIService.exe,,Auto Start,****LocalSystem
Mon Apr 18 15:26:58 2016Z,atapi,,\SystemRoot\system32\drivers\atapi.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,cdrom,,\SystemRoot\system32\drivers\cdrom.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,HpSAMD,,\SystemRoot\system32\drivers\HpSAMD.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,LSI_SAS,,\SystemRoot\system32\drivers\lsi_sas.sys,,Manual,
Mon Apr 18 15:26:58
2016Z,LSI_SCSI,,\SystemRoot\system32\drivers\lsi_scsi.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,MegaSR,,\SystemRoot\system32\drivers\MegaSR.sys,,Manual,

Page 185

SYSTEM OUTPUT.txt
Mon Apr 18 15:26:58 2016Z,msahci,,\SystemRoot\system32\drivers\msahci.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,,Manual,
Mon Apr 18 15:26:58
2016Z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,,Manual,
Mon Apr 18 15:26:58 2016Z,Wd,,\SystemRoot\system32\drivers\wd.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,aliide,,\SystemRoot\system32\drivers\aliide.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,arc,,\SystemRoot\system32\drivers\arc.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,,Manual,
Mon Apr 18 15:26:57
2016Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,LSI_FC,,\SystemRoot\system32\drivers\lsi_fc.sys,,Manual,
Mon Apr 18 15:26:57
2016Z,LSI_SAS2,,\SystemRoot\system32\drivers\lsi_sas2.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,,Manual,
Mon Apr 18 15:26:57
2016Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,,Manual,
Mon Apr 18 15:26:57
2016Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,ST7007,,\SystemRoot\system32\drivers\ST7007.sys,,Manual,
Mon Apr 18 15:26:57
2016Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,,Manual,
Mon Apr 18 15:26:57 2016Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,,Manual,
Mon Apr 18 15:26:55 2016Z,TsUsbGD,Remote Desktop Generic USB
Device,\SystemRoot\system32\drivers\TsUsbGD.sys,,Manual,
Mon Apr 18 15:24:49 2016Z,bcmnfcusb,NFC USB Bus
Driver,\SystemRoot\system32\drivers\bcmnfcusb7.sys,,Manual,
Mon Apr 18 15:23:49 2016Z,ISCT,Intel(R) Smart Connect Technology Device
Driver,\SystemRoot\system32\drivers\ISCTD.sys,,Manual,
Mon Apr 18 15:22:46 2016Z,iwsehub,Intel(R) WSE Hub
Driver,\SystemRoot\system32\drivers\iwsehub.sys,,Manual,
Mon Apr 18 15:22:46 2016Z,iwsepal,Intel(R) WSE-PAL
Driver,\SystemRoot\system32\drivers\iwsepal.sys,,Manual,
Mon Apr 18 15:22:43 2016Z,swmbbnmea05,Sierra Wireless USB Device for NMEA Serial
Communication - Dell,\SystemRoot\system32\drivers\swmbbnmea05.sys,,Manual,
Mon Apr 18 15:22:43 2016Z,swmbbser05,Sierra Wireless USB Device for Serial
Communication - Dell,\SystemRoot\system32\drivers\swmbbser05.sys,,Manual,
Mon Apr 18 15:22:42 2016Z,swg3knmea05,Sierra Wireless QMI NMEA Communication -
Dell,\SystemRoot\system32\drivers\swg3knmea05.sys,,Manual,
Mon Apr 18 15:22:42 2016Z,swg3kser05,Sierra Wireless QMI USB Device for Legacy
Serial Communication - Dell,\SystemRoot\system32\drivers\swg3kser05.sys,,Manual,
Mon Apr 18 15:22:42 2016Z,swibus05,Sierra Wireless Bus Enumerator
05,\SystemRoot\system32\drivers\swibus05.sys,,Manual,
Mon Apr 18 15:22:42 2016Z,swibusflt05,Sierra Wireless Bus Enumerator Filter
05,\SystemRoot\system32\drivers\swibusflt05.sys,,Manual,
Page 186

SYSTEM OUTPUT.txt

Mon Apr 18 15:22:42 2016Z,swimbbbus05,Sierra Wireless MBB Device Bus Enumerator
05,\SystemRoot\system32\drivers\swimbbbus05.sys,,Manual,
Mon Apr 18 15:22:42 2016Z,swimbbbusflt05,Sierra Wireless MBB Device Bus Enumerator
Filter 05,\SystemRoot\system32\drivers\swimbbbusflt05.sys,,Manual,
Wed Dec 30 14:09:15
2015Z,VMBusHID,,\SystemRoot\system32\drivers\VMBusHID.sys,,Manual,
Wed Dec 30 14:08:57 2015Z,tsusbhub,Remote Deskotop USB
Hub,\SystemRoot\system32\drivers\tsusbhub.sys,,Manual,
Wed Dec 30 14:08:56 2015Z,fdc,Floppy Disk Controller
Driver,\SystemRoot\system32\drivers\fdc.sys,,Manual,
Wed Dec 30 14:08:48 2015Z,flpydisk,Floppy Disk
Driver,\SystemRoot\system32\drivers\flpydisk.sys,,Manual,
Wed Dec 30 14:08:47 2015Z,Synth3dVsc,Microsoft Virtual 3D Video Transport
Driver,\SystemRoot\system32\drivers\Synth3dVsc.sys,,Manual,
Wed Dec 30 14:08:18 2015Z,s3cap,,\SystemRoot\system32\drivers\vms3cap.sys,,Manual,
Wed Dec 30 14:05:27
2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\Se
archIndexer.exe /Embedding,,Auto Start,****LocalSystem
Wed Dec 30 14:05:22
2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Wed Dec 30 13:52:01 2015Z,netvsc,,system32\DRIVERS\netvsc60.sys,,Manual,
Wed Dec 30 13:52:01 2015Z,SynthVid,,system32\DRIVERS\VMBusVideoM.sys,,Manual,
Wed Dec 30 13:52:00 2015Z,secdrv,Security Driver,,,Disabled,
Wed Dec 30 13:52:00 2015Z,udfs,udfs,system32\DRIVERS\udfs.sys,,Disabled,
Wed Dec 30 12:33:10
2015Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Auto Start,****LocalSystem
Wed Dec 30 12:27:20
2015Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
regsvc,,Auto Start,****NT AUTHORITY\LocalService
Wed Dec 30 12:27:10
2015Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k bthsvcs,,Disabled,****NT AUTHORITY\LocalService
Wed Dec 30 12:26:59
2015Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k netsvcs,,Disabled,****localSystem
Wed Dec 30 10:09:44 2015Z,amdxata,,system32\drivers\amdxata.sys,,Boot Start,
Wed Dec 30 09:12:34
2015Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k WbioSvcGroup,,Manual,****LocalSystem
Wed Dec 30 07:48:59 2015Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k
GPSvcGroup,,Auto Start,****LocalSystem
Wed Dec 30 07:41:07
2015Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\
svchost.exe -k utcsvc,,Auto Start,****LocalSystem
Wed Dec 30 07:41:07
2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,
Wed Dec 30 07:41:07
2015Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho
st.exe -k LocalService,,Auto Start,****NT AUTHORITY\LocalService
Wed Dec 30 07:41:07
2015Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,
Wed Dec 30 07:41:07 2015Z,iScsiPrt,iScsiPort
Driver,\SystemRoot\system32\drivers\msiscsi.sys,,Manual,
Wed Dec 30 07:41:07 2015Z,terminpt,Microsoft Remote Desktop Input
Driver,\SystemRoot\system32\drivers\terminpt.sys,,Manual,
Wed Dec 30 07:41:07 2015Z,usbcir,eHome Infrared Receiver
(USBCIR),\SystemRoot\system32\drivers\usbcir.sys,,Manual,
Wed Dec 30 07:41:07
2015Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wa
t\WatAdminSvc.exe,,Manual,****LocalSystem
Wed Dec 30 07:41:07

Page 187

SYSTEM OUTPUT.txt

2015Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Wed Dec 30 07:41:07
2015Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Wed Dec 30 07:03:57 2015Z,MSDTC Bridge 3.0.0.0,,,^^^^,,
Wed Dec 30 07:03:57 2015Z,ServiceModelEndpoint 3.0.0.0,,,^^^^,,
Wed Dec 30 07:03:57 2015Z,ServiceModelOperation 3.0.0.0,,,^^^^,,
Wed Dec 30 07:03:57 2015Z,ServiceModelService 3.0.0.0,,,^^^^,,
Wed Dec 30 07:03:57 2015Z,SMSvcHost 3.0.0.0,,,^^^^,,
Wed Dec 30 07:03:57 2015Z,Windows Workflow Foundation 3.0.0.0,,,^^^^,,
Tue Dec 29 15:55:14 2015Z,Microsoft SharePoint Workspace Audit Service,Microsoft
SharePoint Workspace Audit Service,"C:\Program Files (x86)\Microsoft
Office\Office14\GROOVE.EXE" /auditservice,,Manual,****NT AUTHORITY\LocalService
Tue Dec 29 15:55:13 2015Z,Outlook,,,^^^^,,
Tue Dec 29 15:55:12 2015Z,adsi,,,^^^^,,
Tue Dec 29 15:52:10 2015Z,osppsvc,Office Software Protection Platform,"C:\Program
Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",,Manual,****NT
AUTHORITY\NetworkService
Tue Dec 29 15:51:22
2015Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost
.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Dec 29 15:51:11 2015Z,ose,Office  Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",,Manual,****LocalSystem
Tue Apr 12 07:45:41
2011Z,CscService,@%systemroot%\system32\cscsvc.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Apr 12 07:45:24
2011Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k
netsvcs,,Manual,****LocalSystem
Tue Apr 12 07:45:24
2011Z,PeerDistSvc,@%SystemRoot%\system32\peerdistsvc.dll;-9000,%SystemRoot%\System32
\svchost.exe -k PeerDist,,Manual,****NT AUTHORITY\NetworkService
Tue Apr 12 07:45:24 2011Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,,Manual,
Tue Apr 12 07:45:24
2011Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svcho
st.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Apr 12 07:45:24
2011Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Apr 12 07:45:24
2011Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Tue Apr 12 07:45:24 2011Z,VGPU,,System32\drivers\rdvgkmd.sys,,Manual,
Tue Apr 12 07:45:22 2011Z,AppMgmt\Parameters,,%SystemRoot%\System32\appmgmts.dll,,,
Tue Apr 12 07:45:22 2011Z,CscService\Parameters,,%SystemRoot%\System32\cscsvc.dll,,,
Tue Apr 12 07:45:22
2011Z,PeerDistSvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,
Tue Apr 12 07:45:22 2011Z,RDPUDD,,,^^^^,,
Tue Apr 12 07:45:22 2011Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,
Tue Apr 12 07:45:22 2011Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,
Tue Apr 12 07:45:22
2011Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,
Tue Apr 12 07:44:54 2011Z,dmvsc,,\SystemRoot\system32\drivers\dmvsc.sys,,Manual,
Sun Nov 21 03:58:24 2010Z,BTHMODEM,Bluetooth Serial Communications
Driver,\SystemRoot\system32\drivers\bthmodem.sys,,Manual,
Sun Nov 21 03:58:22 2010Z,gagp30kx,Microsoft Generic AGPv3.0 Filter for K8 Processor
Platforms,\SystemRoot\system32\drivers\gagp30kx.sys,,Manual,
Sun Nov 21 03:58:22 2010Z,uagp35,Microsoft AGPv3.5
Filter,\SystemRoot\system32\drivers\uagp35.sys,,Manual,
Sun Nov 21 03:58:21 2010Z,b06bdrv,Broadcom NetXtreme II
Page 188

```
SYSTEM OUTPUT.txt
VBD,\SystemRoot\system32\drivers\bxvbda.sys,,Manual,
Sun Nov 21 03:58:21 2010z,HidBth,Microsoft Bluetooth HID
Miniport,\SystemRoot\system32\drivers\hidbth.sys,,Manual,
Sun Nov 21 03:58:19 2010z,AmdK8,AMD K8 Processor
Driver,\SystemRoot\system32\drivers\amdk8.sys,,Manual,
Sun Nov 21 03:58:19 2010z,AmdPPM,AMD Processor
Driver,\SystemRoot\system32\drivers\amdppm.sys,,Manual,
Sun Nov 21 03:58:19 2010z,Processor,Processor
Driver,\SystemRoot\system32\drivers\processr.sys,,Manual,
Sun Nov 21 03:58:18 2010z,ebdrv,Broadcom NetXtreme II 10 GigE
VBD,\SystemRoot\system32\drivers\evbda.sys,,Manual,
Sun Nov 21 03:58:17 2010z,pcmcia,,\SystemRoot\system32\drivers\pcmcia.sys,,Manual,
Sun Nov 21 03:58:16 2010z,MTConfig,Microsoft Input Configuration
Driver,\SystemRoot\system32\drivers\MTConfig.sys,,Manual,
Sun Nov 21 03:58:15 2010z,circlass,Consumer IR
Devices,\SystemRoot\system32\drivers\circlass.sys,,Manual,
Sun Nov 21 03:58:13 2010z,sffloppy,High-Capacity Floppy Disk
Drive,\SystemRoot\system32\drivers\sffloppy.sys,,Manual,
Sun Nov 21 03:58:11 2010z,HidBatt,HID UPS Battery
Driver,\SystemRoot\system32\drivers\HidBatt.sys,,Manual,
Sun Nov 21 03:58:08 2010z,Hidir,Microsoft Infrared HID
Driver,\SystemRoot\system32\drivers\hidir.sys,,Manual,
Sun Nov 21 03:58:07 2010z,sermouse,Serial Mouse
Driver,\SystemRoot\system32\drivers\sermouse.sys,,Manual,
Sun Nov 21 03:58:06 2010z,BrFiltLo,Brother USB Mass-Storage Lower Filter
Driver,\SystemRoot\system32\drivers\BrFiltLo.sys,,Manual,
Sun Nov 21 03:58:06 2010z,BrFiltUp,Brother USB Mass-Storage Upper Filter
Driver,\SystemRoot\system32\drivers\BrFiltUp.sys,,Manual,
Sun Nov 21 03:58:05 2010z,usbohci,Microsoft USB Open Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbohci.sys,,Manual,
Sun Nov 21 03:58:05 2010z,usbuhci,Microsoft USB Universal Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbuhci.sys,,Manual,
Sun Nov 21 03:58:00 2010z,WacomPen,Wacom Serial Pen HID
Driver,\SystemRoot\system32\drivers\wacompen.sys,,Manual,
Sun Nov 21 03:57:59 2010z,crcdisk,Crcdisk Filter
Driver,\SystemRoot\system32\drivers\crcdisk.sys,,Disabled,
Sun Nov 21 03:57:58 2010z,UmPass,Microsoft UMPass
Driver,\SystemRoot\system32\drivers\umpass.sys,,Manual,
Sun Nov 21 03:57:56 2010z,usbprint,Microsoft USB PRINTER
Class,\SystemRoot\system32\drivers\usbprint.sys,,Manual,
Sun Nov 21 03:46:56 2010z,b57nd60a,Broadcom NetXtreme Gigabit Ethernet - NDIS
6.0,system32\DRIVERS\b57nd60a.sys,,Manual,
Sun Nov 21 03:46:56 2010z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,,Disabled,
Sun Nov 21 03:46:56 2010z,fastfat,FAT12/16/32 File System Driver,,Manual,
Sun Nov 21 03:46:56 2010z,vga,,system32\DRIVERS\vgapnp.sys,,Manual,
Sun Nov 21 03:39:53 2010z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,
Sun Nov 21 03:38:46 2010z,TsUsbFlt,,system32\drivers\tsusbflt.sys,,Manual,
Sun Nov 21 03:33:56
2010z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svch
ost.exe -k netsvcs,,Manual,****localSystem
Sun Nov 21 03:29:32 2010z,1394ohci,1394 OHCI Compliant Host
Controller,\SystemRoot\system32\drivers\1394ohci.sys,,Manual,
Sun Nov 21 03:29:32 2010z,AcpiPmi,ACPI Power Meter
Driver,\SystemRoot\system32\drivers\acpipmi.sys,,Manual,
Sun Nov 21 03:29:32 2010z,agp440,Intel AGP Bus
Filter,\SystemRoot\system32\drivers\agp440.sys,,Manual,
Sun Nov 21 03:29:32 2010z,ErrDev,Microsoft Hardware Error Device
Driver,\SystemRoot\system32\drivers\errdev.sys,,Manual,
Sun Nov 21 03:29:32 2010z,IPMIDRV,,\SystemRoot\system32\drivers\IPMIDrv.sys,,Manual,
Sun Nov 21 03:29:32 2010z,nv_agp,NVIDIA nForce AGP Bus
Filter,\SystemRoot\system32\drivers\nv_agp.sys,,Manual,
Sun Nov 21 03:29:32 2010z,ohci1394,1394 OHCI Compliant Host Controller
Page 189
```

SYSTEM OUTPUT.txt

(Legacy),\SystemRoot\system32\drivers\ohci1394.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffdisk,SFF Storage Class
Driver,\SystemRoot\system32\drivers\sffdisk.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_mmc,SFF Storage Protocol Driver for
MMC,\SystemRoot\system32\drivers\sffp_mmc.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_sd,SFF Storage Protocol Driver for
SDBus,\SystemRoot\system32\drivers\sffp_sd.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,uliagpkx,Uli AGP Bus
Filter,\SystemRoot\system32\drivers\uliagpkx.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,vhdmp,,\SystemRoot\system32\drivers\vhdmp.sys,,Manual,
Tue Jul 14 05:34:12 2009Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,
Tue Jul 14 05:34:12
2009Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,
Tue Jul 14 05:34:12 2009Z,WPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,
Tue Jul 14 05:34:09 2009Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,
Tue Jul 14 05:08:55 2009Z,iphlpsvc\Parameters,,%SystemRoot%\System32\iphlpsvc.dll,,,
Tue Jul 14 04:54:38 2009Z,NdisCap,NDIS Capture LightWeight
Filter,system32\DRIVERS\ndiscap.sys,,Manual,
Tue Jul 14 04:54:32 2009Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,
Tue Jul 14 04:54:31 2009Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,
Tue Jul 14 04:54:25
2009Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,
Tue Jul 14 04:54:05 2009Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,
Tue Jul 14 04:53:57
2009Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,,Manua
l,
Tue Jul 14 04:53:56 2009Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Tue Jul 14 04:53:48 2009Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcss.dll,,,
Tue Jul 14 04:53:45
2009Z,Trkwks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:53:45 2009Z,Trkwks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Tue Jul 14 04:53:36
2009Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:53:36
2009Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Tue Jul 14 04:53:33
2009Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32
\svchost.exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Tue Jul 14 04:53:25 2009Z,WmiApRpl,,,^^^^,,
Tue Jul 14 04:53:24
2009Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****localSystem
Tue Jul 14 04:53:24
2009Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,,Manual,****localSystem
Tue Jul 14 04:53:21 2009Z,TCPIP6,Microsoft IPv6 Protocol
Driver,system32\DRIVERS\tcpip.sys,,Manual,
Tue Jul 14 04:53:21
2009Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,,M
anual,
Tue Jul 14 04:53:20
2009Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:53:19

Page 190

SYSTEM OUTPUT.txt

```
2009Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:53:19 2009Z,Winsock,,,^^^^4,3,
Tue Jul 14 04:49:48
2009Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,,Au
to Start,****LocalSystem
Tue Jul 14 04:49:48
2009Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:46
2009Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:45
2009Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,,Disabled,****localSystem
Tue Jul 14 04:49:45
2009Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Tue Jul 14 04:49:35
2009Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:35 2009Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Tue Jul 14 04:49:35
2009Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
xe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:26 2009Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Tue Jul 14 04:49:24
2009Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:24 2009Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:24
2009Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:24 2009Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:23 2009Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Tue Jul 14 04:49:22 2009Z,TBS\Parameters,,%SystemRoot%\System32\tbssvc.dll,,,
Tue Jul 14 04:49:20 2009Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Tue Jul 14 04:49:18 2009Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Tue Jul 14 04:49:08 2009Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Data,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Networking,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for Oracle,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for SqlServer,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,.NETFramework,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svcho
st.exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,,Manual,
****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\ap
pid.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT Authority\LocalService
```

Page 191

SYSTEM OUTPUT.txt
Tue Jul 14 04:49:01 2009Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\Sys
tem32\svchost.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Tue Jul 14 04:49:01
2009Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Tue Jul 14 04:49:01
2009Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchos
t.exe -k AxInstSVGroup,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,
Tue Jul 14 04:49:01 2009Z,BattC,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,
Tue Jul 14 04:49:01 2009Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,
Tue Jul 14 04:49:01 2009Z,Brserid,Brother MFC Serial Port Interface Driver
(WDM),\SystemRoot\System32\Drivers\Brserid.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrSerWdm,Brother WDM Serial
driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbMdm,Brother MFC USB Fax Only
Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbSer,Brother MFC USB Serial WDM
Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,
Tue Jul 14 04:49:01
2009Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,crypt32,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k NetworkService,,Auto Start,****NT Authority\NetworkService
Tue Jul 14 04:49:01 2009Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,DCLocator,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svch
ost.exe -k defragsvc,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,
Tue Jul 14 04:49:01
2009Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,,Ma
nual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,ESENT,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,
Tue Jul 14 04:49:01 2009Z,exfat,exFAT File System Driver,,,Manual,
Page 192

SYSTEM OUTPUT.txt

Tue Jul 14 04:49:01
2009Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,
Tue Jul 14 04:49:01 2009Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,
Tue Jul 14 04:49:01
2009Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot
%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,,Manual,****NT
Authority\LocalService
Tue Jul 14 04:49:01
2009Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers
\FsDepends.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,hcw85cir,Hauppauge Consumer Infrared
Receiver,\SystemRoot\system32\drivers\hcw85cir.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,
Tue Jul 14 04:49:01
2009Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows
Communication
Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v
3.0\Windows Communication Foundation\infocard.exe",,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,
Tue Jul 14 04:49:01 2009Z,inetaccs,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt
drv.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchos
t.exe -k NetSvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.
sys,,Manual,
Tue Jul 14 04:49:01
2009Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,,Manual,****LocalSyste
m
Tue Jul 14 04:49:01 2009Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,
Tue Jul 14 04:49:01 2009Z,ldap,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.ex
e -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,Lsa,,,^^^^,,
Tue Jul 14 04:49:01

Page 193

SYSTEM OUTPUT.txt
2009Z,MMCSS,@%systemroot%\system32\mmcss.dll;-100,%SystemRoot%\system32\svchost.exe
-k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,MMCSS\Parameters,,%SystemRoot%\system32\mmcss.dll,,,
Tue Jul 14 04:49:01 2009Z,Modem,,system32\drivers\modem.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svc
host.exe -k LocalServiceNoNetwork,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,
Tue Jul 14 04:49:01
2009Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System
32\drivers\mshidkmdf.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchos
t.exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,
Tue Jul 14 04:49:01
2009Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.
exe /V,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,MsRPC,,,,Manual,
Tue Jul 14 04:49:01 2009Z,MSSCNTRS,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.
exe -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,
Tue Jul 14 04:49:01
2009Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,netprofm\Parameters,,%SystemRoot%\System32\netprofm.dll,,,
Tue Jul 14 04:49:01
2009Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,NTDS,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PerfDisk,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,PerfHost,@%systemroot%\syswow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PerfNet,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,PerfOS,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,PerfProc,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,
Tue Jul 14 04:49:01
2009Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchos
t.exe -k DcomLaunch,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
Page 194

SYSTEM OUTPUT.txt
2009Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\sv
chost.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost
.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\sv
chost.exe -k NetworkServiceNetworkRestricted,,Manual,****NT Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PortProxy,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,
Tue Jul 14 04:49:01
2009Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.
exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,ProtectedStorage,@%systemroot%\system32\psbase.dll;-300,%SystemRoot%\system32\
lsass.exe,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,
Tue Jul 14 04:49:01
2009Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\d
rivers\qwavedrv.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,RDPDD,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,^^^^,,
Tue Jul 14 04:49:01
2009Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator
.exe,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,RpcSs,@oleres.dll;-5010,%SystemRoot%\system32\svchost.exe
-k rpcss,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,
Tue Jul 14 04:49:01
2009Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.ex
e -k SDRSVC,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.e
xe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,
Tue Jul 14 04:49:01
2009Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,
Tue Jul 14 04:49:01

Page 195

SYSTEM OUTPUT.txt
2009Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,
Tue Jul 14 04:49:01
2009Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\sv
chost.exe -k netsvcs,,Disabled,****LocalSystem
Tue Jul 14 04:49:01
2009Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,
Tue Jul 14 04:49:01
2009Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System3
2\svchost.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Tue Jul 14 04:49:01
2009Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap
.exe,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.ex
e,^^^^272,2,LocalSystem
Tue Jul 14 04:49:01
2009Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe
,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,sppuinotify,@%SystemRoot%\system32\sppuinotify.dll;-103,%SystemRoot%\system32\
svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,sppuinotify\Parameters,,%SystemRoot%\system32\sppuinotify.dll,,,
Tue Jul 14 04:49:01
2009Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01
2009Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.ex
e -k imgsvc,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Tue Jul 14 04:49:01
2009Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe
-k swprv,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Tue Jul 14 04:49:01
2009Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Tue Jul 14 04:49:01
2009Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchos
t.exe -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Tue Jul 14 04:49:01
2009Z,TBS,@%SystemRoot%\system32\tbssvc.dll;-100,%SystemRoot%\System32\svchost.exe
-k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TCPIP6TUNNEL,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,TCPIPTUNNEL,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,,Manual,****NT Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
Page 196

SYSTEM OUTPUT.txt
host.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Tue Jul 14 04:49:01
2009Z,THREADORDER,@%systemroot%\system32\mmcss.dll;-102,%SystemRoot%\system32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TSDDD,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,UGatherer,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,UGTHRSVC,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,UIODetect,@%SystemRoot%\system32\uiOdetect.exe;-101,%SystemRoot%\system32\UIOD
etect.exe,^^^^272,3,LocalSystem
Tue Jul 14 04:49:01
2009Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Tue Jul 14 04:49:01
2009Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****localSystem
Tue Jul 14 04:49:01 2009Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,
Tue Jul 14 04:49:01
2009Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,,Manual,
****LocalSystem
Tue Jul 14 04:49:01
2009Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,,Man
ual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,W3SVC,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,wbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcssvc,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Tue Jul 14 04:49:01
2009Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,Wecsvc\Parameters,,%SystemRoot%\System32\wecsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Tue Jul 14 04:49:01
2009Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe

Page 197

```
                          SYSTEM OUTPUT.txt
-k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WinSock2,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe",,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\
drivers\ws2ifsl.sys,,Disabled,
Tue Jul 14 04:49:01
2009Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WSearchIdxPi,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Tue Jul 14 04:49:01 2009Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalServiceNoNetwork,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,
Tue Jul 14 04:49:01 2009Z,xmlprov,,,^^^^,,
Tue Jul 14 02:34:41 2009Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Tue Jul 14 02:34:41 2009Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
----------------------------------------
svcdll v.20130603
(System) Lists Services keys with ServiceDll values

Tue Apr 19 19:47:44 2016Z
  EapHost -> %SystemRoot%\System32\eapsvc.dll

Mon Apr 18 16:17:30 2016Z
  Browser -> %SystemRoot%\System32\browser.dll
  HomeGroupListener -> %SystemRoot%\system32\ListSvc.dll
  HomeGroupProvider -> %SystemRoot%\system32\provsvc.dll
  WPCSvc -> %SystemRoot%\System32\wpcsvc.dll

Mon Apr 18 15:30:12 2016Z
  IKEEXT -> %SystemRoot%\System32\ikeext.dll

Mon Apr 18 15:29:32 2016Z
  TabletInputService -> %SystemRoot%\System32\TabSvc.dll

Mon Apr 18 15:29:01 2016Z
  WinDefend -> %ProgramFiles%\Windows Defender\mpsvc.dll

Mon Apr 18 15:28:54 2016Z
  CertPropSvc -> %SystemRoot%\System32\certprop.dll
  SCardSvr -> %SystemRoot%\System32\SCardSvr.dll

Mon Apr 18 15:28:04 2016Z
  Wlansvc -> %SystemRoot%\System32\wlansvc.dll

Wed Dec 30 14:05:22 2015Z
  FDResPub -> %SystemRoot%\system32\fdrespub.dll

Wed Dec 30 12:33:10 2015Z
  BITS -> %SystemRoot%\System32\qmgr.dll
```

Page 198

SYSTEM OUTPUT.txt

```
Wed Dec 30 12:27:20 2015Z
  RemoteRegistry -> %SystemRoot%\system32\regsvc.dll

Wed Dec 30 12:27:10 2015Z
  bthserv -> %SystemRoot%\system32\bthserv.dll

Wed Dec 30 12:26:59 2015Z
  BDESVC -> %SystemRoot%\System32\bdesvc.dll

Wed Dec 30 09:12:34 2015Z
  WbioSrvc -> %SystemRoot%\System32\wbiosrvc.dll

Wed Dec 30 07:48:59 2015Z
  gpsvc -> %SystemRoot%\System32\gpsvc.dll

Wed Dec 30 07:41:07 2015Z
  DiagTrack -> %SystemRoot%\system32\diagtrack.dll
  FontCache -> %SystemRoot%\system32\FntCache.dll
  WebClient -> %SystemRoot%\System32\webclnt.dll
  wudfsvc -> %SystemRoot%\System32\WUDFSvc.dll

Tue Dec 29 15:51:22 2015Z
  wuauserv -> %systemroot%\system32\wuaueng.dll

Tue Apr 12 07:45:41 2011Z
  CscService -> %SystemRoot%\System32\cscsvc.dll

Tue Apr 12 07:45:24 2011Z
  AppMgmt -> %SystemRoot%\System32\appmgmts.dll
  PeerDistSvc -> %SystemRoot%\system32\peerdistsvc.dll
  SensrSvc -> %SystemRoot%\system32\sensrsvc.dll
  StorSvc -> %SystemRoot%\system32\storsvc.dll
  UmRdpService -> %SystemRoot%\System32\umrdp.dll

Sun Nov 21 03:33:56 2010Z
  SessionEnv -> %SystemRoot%\system32\sessenv.dll

Tue Jul 14 04:53:45 2009Z
  TrkWks -> %SystemRoot%\System32\trkwks.dll

Tue Jul 14 04:53:36 2009Z
  RpcEptMapper -> %SystemRoot%\System32\RpcEpMap.dll

Tue Jul 14 04:53:33 2009Z
  LanmanServer -> %SystemRoot%\system32\srvsvc.dll

Tue Jul 14 04:53:31 2009Z
  LanmanWorkstation -> %SystemRoot%\System32\wkssvc.dll

Tue Jul 14 04:53:24 2009Z
  Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll

Tue Jul 14 04:53:20 2009Z
  lmhosts -> %SystemRoot%\System32\lmhsvc.dll

Tue Jul 14 04:53:19 2009Z
  Dhcp -> %SystemRoot%\system32\dhcpcore.dll

Tue Jul 14 04:49:48 2009Z
  W32Time -> %systemroot%\system32\w32time.dll

Tue Jul 14 04:49:46 2009Z
  Dnscache -> %SystemRoot%\System32\dnsrslvr.dll
```

**Page 199**

SYSTEM OUTPUT.txt

Tue Jul 14 04:49:45 2009Z
   RemoteAccess -> %SystemRoot%\System32\mprdim.dll

Tue Jul 14 04:49:35 2009Z
   RasAuto -> %SystemRoot%\System32\rasauto.dll
   RasMan -> %SystemRoot%\System32\rasmans.dll

Tue Jul 14 04:49:24 2009Z
   DPS -> %SystemRoot%\system32\dps.dll
   WdiServiceHost -> %SystemRoot%\system32\wdi.dll
   WdiSystemHost -> %SystemRoot%\system32\wdi.dll

Tue Jul 14 04:49:01 2009Z
   AeLookupSvc -> %SystemRoot%\System32\aelupsvc.dll
   AppIDSvc -> %SystemRoot%\System32\appidsvc.dll
   Appinfo -> %SystemRoot%\System32\appinfo.dll
   AudioEndpointBuilder -> %SystemRoot%\System32\Audiosrv.dll
   AudioSrv -> %SystemRoot%\System32\Audiosrv.dll
   AxInstSV -> %SystemRoot%\System32\AxInstSV.dll
   BFE -> %SystemRoot%\System32\bfe.dll
   CryptSvc -> %SystemRoot%\system32\cryptsvc.dll
   DcomLaunch -> %SystemRoot%\system32\rpcss.dll
   defragsvc -> %Systemroot%\System32\defragsvc.dll
   dot3svc -> %SystemRoot%\System32\dot3svc.dll
   EventSystem -> %systemroot%\system32\es.dll
   fdPHost -> %SystemRoot%\system32\fdPHost.dll
   hidserv -> %SystemRoot%\system32\hidserv.dll
   hkmsvc -> %SystemRoot%\system32\kmsvc.dll
   IPBusEnum -> %SystemRoot%\system32\ipbusenum.dll
   iphlpsvc -> %SystemRoot%\System32\iphlpsvc.dll
   KtmRm -> %systemroot%\system32\msdtckrm.dll
   lltdsvc -> %SystemRoot%\System32\lltdsvc.dll
   MMCSS -> %SystemRoot%\system32\mmcss.dll
   MpsSvc -> %SystemRoot%\system32\mpssvc.dll
   MSiSCSI -> %systemroot%\system32\iscsiexe.dll
   napagent -> %SystemRoot%\system32\qagentRT.dll
   Netman -> %SystemRoot%\System32\netman.dll
   netprofm -> %SystemRoot%\System32\netprofm.dll
   NlaSvc -> %SystemRoot%\System32\nlasvc.dll
   nsi -> %systemroot%\system32\nsisvc.dll
   p2pimsvc -> %SystemRoot%\system32\pnrpsvc.dll
   p2psvc -> %SystemRoot%\system32\p2psvc.dll
   PcaSvc -> %SystemRoot%\System32\pcasvc.dll
   pla -> %systemroot%\system32\pla.dll
   PlugPlay -> %SystemRoot%\system32\umpnpmgr.dll
   PNRPAutoReg -> %SystemRoot%\system32\pnrpauto.dll
   PNRPsvc -> %SystemRoot%\system32\pnrpsvc.dll
   PolicyAgent -> %SystemRoot%\System32\ipsecsvc.dll
   Power -> %SystemRoot%\system32\umpo.dll
   ProfSvc -> %systemroot%\system32\profsvc.dll
   QWAVE -> %windir%\system32\qwave.dll
   RpcSs -> %SystemRoot%\system32\rpcss.dll
   Schedule -> %systemroot%\system32\schedsvc.dll
   SCPolicySvc -> %SystemRoot%\System32\certprop.dll
   SDRSVC -> %Systemroot%\System32\SDRSVC.dll
   seclogon -> %windir%\system32\seclogon.dll
   SENS -> %SystemRoot%\System32\sens.dll
   SharedAccess -> %SystemRoot%\System32\ipnathlp.dll
   ShellHWDetection -> %SystemRoot%\System32\shsvcs.dll
   sppuinotify -> %SystemRoot%\system32\sppuinotify.dll
   SSDPSRV -> %SystemRoot%\System32\ssdpsrv.dll
   SstpSvc -> %SystemRoot%\system32\sstpsvc.dll
                                    Page 200

SYSTEM OUTPUT.txt

```
stisvc -> %SystemRoot%\System32\wiaservc.dll
swprv -> %Systemroot%\System32\swprv.dll
SysMain -> %systemroot%\system32\sysmain.dll
TapiSrv -> %SystemRoot%\System32\tapisrv.dll
TBS -> %SystemRoot%\System32\tbssvc.dll
TermService -> %SystemRoot%\System32\termsrv.dll
Themes -> %SystemRoot%\system32\themeservice.dll
THREADORDER -> %SystemRoot%\system32\mmcss.dll
upnphost -> %SystemRoot%\System32\upnphost.dll
UxSms -> %SystemRoot%\System32\uxsms.dll
wcncsvc -> %SystemRoot%\System32\wcncsvc.dll
WcsPlugInService -> %SystemRoot%\System32\WcsPlugInService.dll
wecsvc -> %SystemRoot%\system32\wecsvc.dll
wercplsupport -> %SystemRoot%\System32\wercplsupport.dll
WerSvc -> %SystemRoot%\System32\WerSvc.dll
WinHttpAutoProxySvc -> winhttp.dll
WinRM -> %SystemRoot%\system32\WsmSvc.dll
WPDBusEnum -> %SystemRoot%\system32\wpdbusenum.dll
wscsvc -> %SystemRoot%\System32\wscsvc.dll
WwanSvc -> %SystemRoot%\System32\wwansvc.dll
```

----------------------------------------
ControlSet001\Control\Terminal Server
LastWrite Time Wed Apr 20 15:40:55 2016 (UTC)

Reference: http://support.microsoft.com/kb/243215

   ProductVersion = 5.1

   fDenyTSConnections = 0
   1 = connections denied


   TSAdvertise = 0
   0 = disabled, 1 = enabled (advertise Terminal Services)
   Ref: http://support.microsoft.com/kb/281307


   TSUserEnabled = 0
   1 = All users logging in are automatically part of the
   built-in Terminal Server User group. 0 = No one is a
   member of the built-in group.
   Ref: http://support.microsoft.com/kb/238965

AutoStart Locations
Wds\rdpwd key
   StartupPrograms: rdpclip
Analysis Tip: This value usually contains 'rdpclip'; any additional entries
should be investigated.

WinStations\RDP-Tcp key
   InitialProgram: {blank}
Analysis Tip: Maybe be empty; appears as '{blank}'

WinStations\RDP-Tcp key
   UserAuthentication: 0
Analysis Tip: If the UserAuthentication value is 0, the system may be
susceptible to a priv escalation exploitation via Sticky Keys.  See:
http://www.room362.com/blog/2012/5/25/sticky-keys-and-utilman-against-nla.html
----------------------------------------
timezone v.20130830
(System) Get TimeZoneInformation key contents

Page 201

SYSTEM OUTPUT.txt

```
TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Mon Apr 18 16:26:45 2016 (UTC)
  DaylightName    -> @tzres.dll,-111
  StandardName    -> @tzres.dll,-112
  Bias            -> 300 (5 hours)
  ActiveTimeBias -> 240 (4 hours)
-------------------------------------------
usb v.20141111
(System) Get USB key info


USBStor
ControlSet001\Enum\USB

ROOT_HUB20 [Mon Apr 18 15:26:48 2016]
  S/N: 4&1602b482&0 [Wed Apr 20 15:40:49 2016]
  Device Parameters LastWrite: [Mon Apr 18 15:29:05 2016]
  LogConf LastWrite          : [Mon Apr 18 15:26:48 2016]
  Properties LastWrite       : [Mon Apr 18 15:27:43 2016]
    ParentIdPrefix: 5&2726e048&0
    InstallDate     : Mon Apr 18 15:27:44 2016 UTC
    FirstInstallDate: Mon Apr 18 15:27:44 2016 UTC

VID_046D&PID_C52B [Wed Apr 20 12:56:27 2016]
  S/N: 7&11f2eb4f&0&3 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 12:56:27 2016]
  LogConf LastWrite          : [Wed Apr 20 12:56:27 2016]
  Properties LastWrite       : [Wed Apr 20 12:56:45 2016]
    ParentIdPrefix: 8&370ce34f&0
    InstallDate     : Wed Apr 20 12:56:48 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:48 2016 UTC

VID_046D&PID_C52B&MI_00 [Wed Apr 20 12:56:27 2016]
  S/N: 8&370ce34f&0&0000 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 12:56:27 2016]
  LogConf LastWrite          : [Wed Apr 20 12:56:27 2016]
  Properties LastWrite       : [Wed Apr 20 12:56:37 2016]
    ParentIdPrefix: 9&10301e74&0
    InstallDate     : Wed Apr 20 12:56:37 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:37 2016 UTC

VID_046D&PID_C52B&MI_01 [Wed Apr 20 12:56:27 2016]
  S/N: 8&370ce34f&0&0001 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 12:56:27 2016]
  LogConf LastWrite          : [Wed Apr 20 12:56:27 2016]
  Properties LastWrite       : [Wed Apr 20 12:56:35 2016]
    ParentIdPrefix: 9&13a71f4e&0
    InstallDate     : Wed Apr 20 12:56:35 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:35 2016 UTC

VID_046D&PID_C52B&MI_02 [Wed Apr 20 12:56:27 2016]
  S/N: 8&370ce34f&0&0002 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 12:56:27 2016]
  LogConf LastWrite          : [Wed Apr 20 12:56:27 2016]
  Properties LastWrite       : [Wed Apr 20 12:56:49 2016]
    ParentIdPrefix: 9&377e5d10&0
    InstallDate     : Wed Apr 20 12:56:49 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:49 2016 UTC

VID_04F3&PID_032D [Mon Apr 18 15:29:24 2016]
  S/N: 5&13be0f17&0&5 [Mon Apr 18 15:28:31 2016]
  Device Parameters LastWrite: [Mon Apr 18 15:28:30 2016]
  LogConf LastWrite          : [Mon Apr 18 15:26:54 2016]
```

Page 202

```
                              SYSTEM OUTPUT.txt
   Properties LastWrite         : [Mon Apr 18 15:28:30 2016]
     ParentIdPrefix: 6&12a450b0&0
     InstallDate     : Mon Apr 18 15:28:31 2016 UTC
     FirstInstallDate: Mon Apr 18 15:28:31 2016 UTC
   S/N: 6&18876750&0&5 [Wed Apr 20 15:40:51 2016]
   Device Parameters LastWrite: [Mon Apr 18 15:29:31 2016]
   LogConf LastWrite           : [Mon Apr 18 15:29:24 2016]
   Properties LastWrite        : [Mon Apr 18 15:29:32 2016]
     ParentIdPrefix: 7&191fcc70&0
     InstallDate     : Mon Apr 18 15:29:32 2016 UTC
     FirstInstallDate: Mon Apr 18 15:29:32 2016 UTC

 VID_058F&PID_6387 [Tue Apr 19 19:48:22 2016]
   S/N: B57D6A2F [Tue Apr 19 20:53:18 2016]
   Device Parameters LastWrite: [Tue Apr 19 19:48:24 2016]
   LogConf LastWrite           : [Tue Apr 19 19:48:22 2016]
   Properties LastWrite        : [Tue Apr 19 19:48:22 2016]
     InstallDate     : Tue Apr 19 19:48:24 2016 UTC
     FirstInstallDate: Tue Apr 19 19:48:24 2016 UTC

 VID_09C3&PID_0013 [Wed Apr 20 12:56:27 2016]
   S/N: 7&11f2eb4f&0&1 [Wed Apr 20 15:40:52 2016]
   Device Parameters LastWrite: [Wed Apr 20 15:41:00 2016]
   LogConf LastWrite           : [Wed Apr 20 12:56:27 2016]
   Properties LastWrite        : [Wed Apr 20 12:56:43 2016]
     ParentIdPrefix: 8&311b6d2&0
     InstallDate     : Wed Apr 20 12:56:45 2016 UTC
     FirstInstallDate: Wed Apr 20 12:56:45 2016 UTC

 VID_0A5C&PID_5800 [Mon Apr 18 15:26:54 2016]
   S/N: 0123456789ABCD [Wed Apr 20 15:40:52 2016]
   Device Parameters LastWrite: [Mon Apr 18 15:29:03 2016]
   LogConf LastWrite           : [Mon Apr 18 15:26:54 2016]
   Properties LastWrite        : [Mon Apr 18 15:28:49 2016]
     ParentIdPrefix: 7&66de6c9&0
     InstallDate     : Mon Apr 18 15:28:50 2016 UTC
     FirstInstallDate: Mon Apr 18 15:28:50 2016 UTC

 VID_0A5C&PID_5800&MI_00 [Mon Apr 18 15:26:54 2016]
   S/N: 7&66de6c9&0&0000 [Wed Apr 20 15:40:52 2016]
   Device Parameters LastWrite: [Mon Apr 18 15:29:03 2016]
   LogConf LastWrite           : [Mon Apr 18 15:26:54 2016]
   Properties LastWrite        : [Mon Apr 18 15:28:52 2016]
     InstallDate     : Mon Apr 18 15:28:52 2016 UTC
     FirstInstallDate: Mon Apr 18 15:28:52 2016 UTC

 VID_0A5C&PID_5800&MI_01 [Mon Apr 18 15:26:54 2016]
   S/N: 7&66de6c9&0&0001 [Wed Apr 20 15:40:52 2016]
   Device Parameters LastWrite: [Wed Apr 20 15:41:01 2016]
   LogConf LastWrite           : [Mon Apr 18 15:26:54 2016]
   Properties LastWrite        : [Mon Apr 18 15:28:52 2016]
     ParentIdPrefix: 8&38de34d8&0
     InstallDate     : Mon Apr 18 15:28:55 2016 UTC
     FirstInstallDate: Mon Apr 18 15:28:55 2016 UTC

 VID_1BCF&PID_2B8D [Mon Apr 18 15:26:54 2016]
   S/N: 6&18876750&0&6 [Wed Apr 20 15:40:51 2016]
   Device Parameters LastWrite: [Mon Apr 18 15:29:00 2016]
   LogConf LastWrite           : [Mon Apr 18 15:26:54 2016]
   Properties LastWrite        : [Mon Apr 18 15:28:50 2016]
     ParentIdPrefix: 7&38b255c6&0
     InstallDate     : Mon Apr 18 15:28:51 2016 UTC
     FirstInstallDate: Mon Apr 18 15:28:51 2016 UTC
                              Page 203
```

SYSTEM OUTPUT.txt

```
VID_1BCF&PID_2B8D&MI_00 [Mon Apr 18 15:26:54 2016]
  S/N: 7&38b255c6&0&0000 [Wed Apr 20 15:40:52 2016]
  Device Parameters LastWrite: [Mon Apr 18 15:28:57 2016]
  LogConf LastWrite           : [Mon Apr 18 15:26:54 2016]
  Properties LastWrite        : [Mon Apr 18 15:28:57 2016]
    FriendlyName    : Integrated Webcam
    InstallDate     : Mon Apr 18 15:28:57 2016 UTC
    FirstInstallDate: Mon Apr 18 15:28:57 2016 UTC

VID_413C&PID_2513 [Wed Apr 20 12:56:26 2016]
  S/N: 6&18876750&0&1 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 14:27:07 2016]
  LogConf LastWrite           : [Wed Apr 20 12:56:25 2016]
  Properties LastWrite        : [Wed Apr 20 12:56:33 2016]
    InstallDate     : Wed Apr 20 12:56:34 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:34 2016 UTC
  S/N: 6&18876750&0&4 [Wed Apr 20 16:36:48 2016]
  Device Parameters LastWrite: [Wed Apr 20 14:27:07 2016]
  LogConf LastWrite           : [Wed Apr 20 12:56:26 2016]
  Properties LastWrite        : [Wed Apr 20 12:56:39 2016]
    ParentIdPrefix: 7&11f2eb4f&0
    InstallDate     : Wed Apr 20 12:56:42 2016 UTC
    FirstInstallDate: Wed Apr 20 12:56:42 2016 UTC

VID_8087&PID_0A2A [Mon Apr 18 15:26:53 2016]
  S/N: 6&18876750&0&3 [Mon Apr 18 15:34:46 2016]
  Device Parameters LastWrite: [Mon Apr 18 15:29:35 2016]
  LogConf LastWrite           : [Mon Apr 18 15:26:53 2016]
  Properties LastWrite        : [Mon Apr 18 15:28:51 2016]
    ParentIdPrefix: 7&316d53d2&0
    InstallDate     : Mon Apr 18 15:28:51 2016 UTC
    FirstInstallDate: Mon Apr 18 15:28:51 2016 UTC

VID_8087&PID_8001 [Mon Apr 18 15:26:53 2016]
  S/N: 5&2726e048&0&1 [Wed Apr 20 15:40:50 2016]
  Device Parameters LastWrite: [Mon Apr 18 15:29:05 2016]
  LogConf LastWrite           : [Mon Apr 18 15:26:53 2016]
  Properties LastWrite        : [Mon Apr 18 15:26:59 2016]
    ParentIdPrefix: 6&18876750&0
    InstallDate     : Mon Apr 18 15:27:01 2016 UTC
    FirstInstallDate: Mon Apr 18 15:27:01 2016 UTC

-------------------------------------------
usbdevices v.20140416
(System) Parses Enum\USB key for USB & WPD devices

VID_058F&PID_6387
LastWrite: Tue Apr 19 19:48:22 2016
  SN         : B57D6A2F
  LastWrite: Tue Apr 19 20:53:18 2016

-------------------------------------------
usbstor v.20141111
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_&Prod_&Rev_8.07 [Tue Apr 19 19:48:24 2016]
  S/N: B57D6A2F&0 [Tue Apr 19 19:48:25 2016]
  Device Parameters LastWrite: [Tue Apr 19 19:48:25 2016]
  LogConf LastWrite           : [Tue Apr 19 19:48:24 2016]
```

```
                            SYSTEM OUTPUT.txt
   Properties LastWrite       : [Tue Apr 19 19:48:25 2016]
     FriendlyName    : USB Device
     InstallDate     : Tue Apr 19 19:48:25 2016 UTC
     FirstInstallDate: Tue Apr 19 19:48:25 2016 UTC


-----------------------------------
OCL0166192,Disk&Ven_&Prod_&Rev_8.07,B57D6A2F&0,1461095305,USB Device
-----------------------------------
Disk&Ven_&Prod_&Rev_8.07,Tue Apr 19 19:48:24 2016,B57D6A2F&0,Tue Apr 19 19:48:25
2016,USB Device,
-----------------------------------
xpedition v.20120722
(System) Queries System hive for XP Edition info

xpedition v.20120722
-----------------------------------
wpdbusenum v.20141111
(System) Get WpdBusEnumRoot subkey info

DISK&VEN_&PROD_&REV_8.07 (B57D6A2F&0)
   LastWrite: Tue Apr 19 19:48:27 2016
   DeviceDesc:
   Friendly: Configuration Manager 2012
   Mfg:
   Device Parameters LastWrite: [Tue Apr 19 20:53:20 2016]
   LogConf LastWrite          : [Tue Apr 19 19:48:26 2016]
   Properties LastWrite       : [Tue Apr 19 19:48:27 2016]
   InstallDate     : Tue Apr 19 19:48:27 2016 UTC
   FirstInstallDate: Tue Apr 19 19:48:27 2016 UTC

ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
DISK&VEN_&PROD_&REV_8.07\B57D6A2F&0
LastWrite: Tue Apr 19 19:48:27 2016


-----------------------------------
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe
WARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:
pssogina.dll
Alert: svc: AdobeFlashPlayerUpdateSvc has a WOW64 value: 1
Alert: svc: atashost has a WOW64 value: 1
Alert: svc: clr_optimization_v2.0.50727_32 has a WOW64 value: 1
Alert: svc: CVPNDRVA has a WOW64 value: 1
Alert: svc: gupdate has a WOW64 value: 1
Alert: svc: gupdatem has a WOW64 value: 1
Alert: svc: MozillaMaintenance has a WOW64 value: 1
Alert: svc: PerfHost has a WOW64 value: 1
Alert: svc: WIMMount has a WOW64 value: 1
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll
```

Page 205

MD-JICRIM 4:29.6, MPJI-Cr 4:29.6

Maryland Criminal Pattern Jury Instructions
CHAPTER FOUR CRIMINAL OFFENSES

Maryland State Bar Standing Committee on Pattern Jury Instructions

2nd Edition, 2016 Supplement

MPJI-Cr 4:29.6 SEXUAL OFFENSES -- SECOND DEGREE SEXUAL OFFENSE (AGE)

**The defendant is charged with the crime of second degree sexual offense. In order to convict the defendant of second degree sexual offense, the State must prove:**
**(1) that the defendant committed [fellatio] [cunnilingus] [analingus] [anal intercourse] with (name);**

**(2) that (name) was under fourteen years of age at the time of the act; and**

**(3) that the defendant was then at least four years older than (name).**

**Fellatio means that [the defendant applied [his] [her] mouth to the sexual organ of a male] [another applied [his] [her] mouth to the sexual organ of the male defendant].**

**Cunnilingus means that [the defendant applied [his] [her] mouth to the sexual organ of a female] [another applied [his] [her] mouth to the sexual organ of the female defendant].**

**Analingus means that [the defendant applied [his] [her] mouth to the anus of another] [another applied [his] [her] mouth to the anus of the defendant].**

**Anal intercourse means that [the defendant placed his penis into the anus of another, even the slightest amount] [another placed his penis into the anus of the defendant, even the slightest amount].**

### Notes on Use

Use this instruction if the defendant is charged with second degree sexual offense under Md. Code Ann., Crim. Law I § 3-306(a)(3) (2012). In (1), use only the sexual act(s) for which a prima facie case has been established. Similarly, use only the definitional paragraph(s) for the sexual act(s) for which a prima facie case has been established. If there is evidence that the sexual act was consensual, the Committee recommends that the court add: "If all the elements of the offense are proven, it is not a defense that the victim consented to the act of [fellatio] [cunnilingus] [analingus] [anal intercourse]."

### Comment

*See* Comments to MPJI-Cr 4:29.3 (Sexual Offenses -- Second Degree Rape (Age)) and MPJI-Cr 4:29.4 (Sexual Offenses -- Second Degree Sexual Offense).

Second degree sexual offense includes strict liability for a sexual act with a victim less than fourteen years of age by a defendant at least four years older than the victim. Md. Code Ann., Crim. Law I § 3-306(a)(3) (2012); *see Scott v. State*, 43 Md. App. 323, 324-26, 405 A.2d 320, 321-22 (1979) (finding that a birth certificate establishing that the victim was under fourteen at the time of the incident was sufficient to establish the victim's age when the crime was committed, even though the certificate contradicted the victim's testimony, and the mother was uncertain of the year of the victim's birth) *modified on other grounds*, 289 Md. 647, 426 A.2d 923 (1981).

Copyright © 2016 The Maryland State Bar Association, Inc.

---

**End of Document**

© 2017 Thomson Reuters. No claim to original U.S. Government Works.

Admin OUTPUT.txt

acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
--------------------------------------------
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
--------------------------------------------

Acer

aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install

Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
--------------------------------------------
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.

Software\SmartLine Vision\aports not found.

--------------------------------------------
appcompatflags v.20130930
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.

Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
LastWrite Time Thu Mar 24 13:29:24 2016 (UTC)

C:\Program Files (x86)\Encore\Hoyle Puzzle and Board Games 2011\Hoyle Puzzle
Games.exe -> DWM8And16BitMitigation

Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Store
  Fri Jul 10 10:59:56 2015 - C:\OEM\Preload\DPOP\OEMCustomize\FirstBoot.cmd
  Fri Jul 10 10:59:56 2015 - C:\Program Files\Acer\Acer Quick Access\QAAgent.exe
  Fri Jul 10 11:00:24 2015 - C:\OEM\Preload\Autorun\CheckFiles.exe
  Fri Jul 10 11:00:24 2015 - SIGN.MEDIA=736AE setup.exe
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Microsoft\OneDrive\17.3.5892.0626\FileSyncConfig.ex
e
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Microsoft\OneDrive\17.3.6302.0225\FileSyncConfig.ex
e
  Fri Jul 10 11:00:24 2015 - SIGN.MEDIA=8377A2FC HoylePuzzleGames2011.exe
  Fri Jul 10 10:59:56 2015 - C:\Program Files\mcafee.com\agent\mcagent.exe
  Fri Jul 10 11:00:24 2015 - SIGN.MEDIA=4C872 Autoplay.exe
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\Setup_serial__4e4lsIelYA82RIS2XslUA2_key.exe
  Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Microsoft
Office\Office15\FIRSTRUN.EXE
  Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Microsoft
Office\Office12\POWERPNT.EXE
  Fri Jul 10 11:00:24 2015 - C:\Users\DeputyGod\Downloads\mbam-setup-2.2.1.1043.exe
  Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbam.exe
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\MFC-9340CDW-inst-B1-ASA.EXE
  Fri Jul 10 11:00:24 2015 - C:\Program Files
(x86)\Browny02\Brother\BrotherUSBTool.exe
  Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\HMA-Pro-VPN-2.8.24.0-install.exe
                              Page 1

Admin OUTPUT.txt
```
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\HMA! Pro VPN\bin\HMA! Pro
VPN.exe
   Fri Jul 10 11:00:24 2015 - C:\Users\DeputyGod\Downloads\JavaSetup8u73.exe
   Fri Jul 10 10:59:56 2015 - C:\Program Files\Internet Explorer\iexplore.exe
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\flashplayer21_ha_install.exe
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\Shockwave_Installer_Slim.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Acer\abDocs\AcerDocsSetup.exe
   Fri Jul 10 10:59:56 2015 - C:\Program Files (x86)\Acer\abFiles\abFilesSetup.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Adobe\Photoshop Elements
2\PhotoshopElements.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files
(x86)\Brother\BrLauncher\BrLauncher.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Encore\Hoyle Puzzle and Board
Games 2011\Hoyle Puzzle Games.exe
   Fri Jul 10 11:00:24 2015 - C:\Users\DeputyGod\Downloads\yahoo_messenger.exe
   Fri Jul 10 11:00:24 2015 - C:\Users\DeputyGod\Downloads\msgr11us.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files
(x86)\Yahoo!\Messenger\YahooMessenger.exe
   Fri Jul 10 11:00:24 2015 - C:\Users\DeputyGod\Downloads\mbae-setup-1.08.1.1189.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Microsoft
Office\Office12\WINWORD.EXE
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Temp\{111CEF29-CDE8-4CC6-BBC7-ACA372BF2ED0}\Install
FlashPlayer.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Yahoo!\Common\unyt_wrap.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files
(x86)\Yahoo!\SoftwareUpdate\Uninst_AutoUpdater.exe
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Yahoo!\Messenger\UNWISE.EXE
   Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Mozilla Firefox\firefox.exe
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\Downloads\Setup_serial_CoG3vb33Faf19yZQNPOuRg2_key.exe
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Temp\McInstallTemp\Install.exe
   Fri Jul 10 10:59:56 2015 - C:\Program Files\McAfee\MSC\mcsync.exe
   Fri Jul 10 11:00:24 2015 -
C:\Users\DeputyGod\AppData\Local\Temp\jre-8u91-windows-au.exe
-------------------------------------
applets v.20140723
(NTUSER.DAT) Gets contents of user's Applets key

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Tue Mar 22 13:17:28 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
-------------------------------------
Software\Microsoft\IntelliPoint\AppSpecific not found.
-------------------------------------
Software\Ares not found.
-------------------------------------
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
-------------------------------------
autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task

Control Panel\Desktop

AutoEndTasks value not found.
```
Page 2

Admin OUTPUT.txt
------------------------------------
autorun v.20081212
(NTUSER.DAT) Gets autorun settings

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer not found.
------------------------------------
bitbucket_user v.20091020
(NTUSER.DAT) TEST - Get user BitBucket values

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Tue Mar 22 13:17:31 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume
LastWrite Time = Tue Mar 22 13:14:51 2016 (UTC)

------------------------------------
brisv v.20130429
(NTUSER.DAT) Detect artifacts of a Troj.Brisv.A infection

Software\Microsoft\PIMSRV not found.
------------------------------------
cain v.20110204
(NTUSER.DAT) Extracts details for Cain & Abel by oxid.it

Software\Cain\Settings not found.

------------------------------------
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.

------------------------------------
clampi v.20091019
(NTUSER.DAT) TEST - Checks for keys set by Trojan.Clampi PROT module

Software\Microsoft\Internet Explorer\Main
LastWrite Time Fri Mar 25 06:10:49 2016 (UTC)


Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete not found.

Software\Microsoft\Internet Account Manager\Accounts not found.

The system does not appear to have been infected with the Trojan.Clampi
PROT module.
------------------------------------
clampitm v.20100624
(NTUSER.DAT) Checks for IOCs for Clampi (per Trend Micro)

ClampiTM plugin
Software\Microsoft\Internet Explorer\Settings
LastWrite Time Tue Mar 22 13:13:02 2016 (UTC)

No Clampi values found.
------------------------------------
comdlg32 v.20121008

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time Thu Mar 24 13:04:27 2016 (UTC)
CIDSizeMRU
LastWrite: Thu Apr 21 04:39:41 2016
Note: All value names are listed in MRUListEx order.
Page 3

Admin OUTPUT.txt

YahooMessenger.exe
firefox.exe
YAHOOM~1.EXE
PhotoshopElements.exe
{90CCAB49-A3A8-423A-868B-03DD4B3F11BC}
SnippingTool.exe

FirstFolder
LastWrite: Sat Mar 26 04:58:54 2016
Note: All value names are listed in MRUListEx order.

   C:\Program Files (x86)\Yahoo!\Messenger\YahooMessenger.exe
   C:\PROGRA~2\Yahoo!\MESSEN~1\YAHOOM~1.EXE
   C:\Program Files (x86)\Adobe\Photoshop Elements 2\PhotoshopElements.exe

LastVisitedPidlMRU
LastWrite: Thu Apr 21 04:39:41 2016
Note: All value names are listed in MRUListEx order.

   YahooMessenger.exe - My Computer\Unknown Type (0x2e)\.\.\.
   firefox.exe - My Computer\Unknown Type (0x2e)\.\.\.
   YAHOOM~1.EXE - My Computer\Unknown Type (0x2e)
   {90CCAB49-A3A8-423A-868B-03DD4B3F11BC} - My Computer\C:\.\.\.

LastVisitedPidlMRU
LastWrite: Tue Apr 12 22:18:04 2016
Note: All value names are listed in MRUListEx order.

   YAHOOM~1.EXE - My Computer\Unknown Type (0x2e)\.\.
   YahooMessenger.exe - My Computer\Unknown Type (0x2e)\.\.\.\.
   PhotoshopElements.exe - My Computer\Unknown Type (0x2e)\.\.

OpenSavePidlMRU
LastWrite: Tue Apr 12 22:10:57 2016
OpenSavePidlMRU\*
LastWrite Time: Thu Apr 21 04:39:41 2016
Note: All value names are listed in MRUListEx order.

   My Computer\Unknown Type (0x2e)\.\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.
   My Computer\Unknown Type (0x2e)\.\.\.

OpenSavePidlMRU\docx
LastWrite Time: Tue Mar 29 12:24:53 2016
Note: All value names are listed in MRUListEx order.

Page 4

Admin OUTPUT.txt

My Computer\C:\.\.\.\.\.

OpenSavePidlMRU\jpg
LastWrite Time: Thu Apr 21 04:39:41 2016
Note: All value names are listed in MRUListEx order.

My Computer\Unknown Type (0x2e)\.\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.
My Computer\Unknown Type (0x2e)\.\.\.\.

OpenSavePidlMRU\mp4
LastWrite Time: Tue Apr 12 22:10:57 2016
Note: All value names are listed in MRUListEx order.

My Computer\Unknown Type (0x2e)\.

------------------------------------------
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted not found.
------------------------------------------
compdesc v.20080324
(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions not found.
------------------------------------------
controlpanel v.20080428
(NTUSER.DAT) Look for RecentTask* values in ControlPanel key (Vista)

Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel not found.
------------------------------------------
cpldontload v.20100116
(NTUSER.DAT) Gets contents of user's Control Panel don't load key

Control Panel\don't load
LastWrite Time Tue Mar 22 13:17:42 2016 (UTC)

Control Panel\don't load has no values.
------------------------------------------
decaf v.20110210
(NTUSER.DAT) Extracts the EULA value for DECAF.

Software\DECAFme not found.

------------------------------------------
Page 5

Admin OUTPUT.txt

dependency_walker v.20110204
(NTUSER.DAT) Extracts Recent File List for Dependency Walker.

Software\Microsoft\Dependency Walker\Recent File List not found.

----------------------------------------
domains v.20100116
(NTUSER.DAT) Gets contents Internet Settings\ZoneMap\Domains key

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
LastWrite Time Tue Mar 22 13:13:18 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap has no subkeys.
----------------------------------------
environment v.20110204
(NTUSER.DAT) Extracts user's Environment paths from NTUSER.DAT

Environment
Environment
LastWrite Time Wed Mar 23 10:11:11 2016 (UTC)

TEMP -> %USERPROFILE%\AppData\Local\Temp
TMP -> %USERPROFILE%\AppData\Local\Temp
PATH -> C:\Program Files (x86)\HMA! Pro VPN\bin

----------------------------------------
fileexts v.20080818
(NTUSER.DAT) Get user FileExts values

fileexts
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

----------------------------------------
filehistory v.20120620
(NTUSER.DAT) Gets filehistory settings

Software\Microsoft\Windows\CurrentVersion\FileHistory
LastWrite Time Tue Mar 22 13:13:02 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\FileHistory has no values.
File History may not be configured for this user.
----------------------------------------
gthist v.20100218
(NTUSER.DAT) Gets Google Toolbar Search History

Software\Google\NavClient\1.1\History not found.
----------------------------------------
gtwhitelist v.20100218
(NTUSER.DAT) Gets Google Toolbar whitelist values

Software\Google\Google Toolbar\4.0\whitelist not found.
----------------------------------------
haven_and_hearth v.20110204
(NTUSER.DAT) Extracts the username and savedtoken for Haven & Hearth.

Software\JavaSoft\Prefs\haven not found.

----------------------------------------
ie_settings v.20130731
(NTUSER.DAT) Gets important user IE settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 12 20:55:36 2016 (UTC)

Page 6

Admin OUTPUT.txt

```
User Agent = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade = Tue Mar 22 13:13:18 2016 (UTC)
DaysToKeep value not found - default is 20 days

Software\Microsoft\Internet Explorer\Main\WindowsSearch
LastWrite Time Wed Mar 23 10:24:33 2016 (UTC)
Version = 10.0.10240.16431

'Cleared' value not found.

UpgradeTime = Wed Mar 23 08:52:53 2016 UTC
User Favorites Path = file:///C:\Users\DeputyGod\Favorites\
-----------------------------------------
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Fri Mar 25 06:10:45 2016 (UTC)
  Download Directory = ''

Software\Microsoft\Internet Explorer\AutoComplete not found.

Software\Microsoft\Internet Explorer\DOMStorage
LastWrite Time Fri Apr 15 00:51:39 2016 (UTC)
Subkeys:
  ad.doubleclick.net       ---  Fri Mar 25 16:20:38 2016 UTC
  advertising.com          ---  Tue Apr 12 20:47:12 2016 UTC
  betrad.com               ---  Sun Apr  3 19:13:33 2016 UTC
  c.betrad.com             ---  Sun Apr  3 19:13:33 2016 UTC
  doubleclick.net          ---  Fri Mar 25 16:20:38 2016 UTC
  insider.msg.yahoo.com --- Tue Apr  5 21:15:13 2016 UTC
  malwarebytes.org         ---  Sun Mar 27 08:58:28 2016 UTC
  na.ads.yahoo.com         ---  Sun Apr  3 00:44:04 2016 UTC
  Total                    ---  Tue Apr  5 21:15:13 2016 UTC
  w55c.net                 ---  Fri Apr 15 00:51:39 2016 UTC
  www.malwarebytes.org --- Sun Mar 27 08:58:28 2016 UTC
  yahoo.com                ---  Tue Apr  5 21:15:13 2016 UTC

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Tue Mar 22 13:13:18 2016 (UTC)
  Internet Explorer version = 0.0.0.0

Software\Microsoft\Internet Explorer\Main
LastWrite Time Fri Mar 25 06:10:49 2016 (UTC)
  Anchor Underline                        = yes
  ApplicationTileImmersiveActivation      = 0
  AssociationActivationMode               = 2
  Cache_Update_Frequency                  = yes
  CompatibilityFlags                      = 0 [0x00000000]
  Default_Page_URL                        = http://acer15.msn.com/?pc=ACTE
  Disable Script Debugger                 = yes
  DisableFirstRunCustomize                = 1
  DisableScriptDebuggerIE                 = yes
  Display Inline Images                   = yes
  Do404Search                             = 1 [0x01000000]
  EdgeSwitchingOSBuildNumber              = 10240.th1_st1.150717-1719
  Enable Browser Extensions               = yes
  FullScreen                              = no
  ImageStoreRandomFolder                  = ycxmbxy
  Local Page                              = %11%\blank.htm
  OperationalData                         =
```

Page 7

```
                                  Admin OUTPUT.txt
   Play_Animations                          = yes
   Play_Background_Sounds                   = yes
   Save_Session_History_On_Exit            = no
   Search Page                             =
http://go.microsoft.com/fwlink/?LinkId=54896
   Show_FullURL                            = no
   Show_StatusBar                          = yes
   Show_ToolBar                            = yes
   Show_URLToolBar                         = yes
   Show_URLinStatusBar                     = yes
   Start Page                              = http://acer15.msn.com/?pc=ACTE
   UseClearType                            = no
   Use_DlgBox_Colors                       = yes
   Window_Placement                        = <skipped>
   XMLHTTP                                 = true   [1]


   Software\Microsoft\Internet Explorer\Main\WindowsSearch
   LastWrite Time Wed Mar 23 10:24:33 2016 (UTC)
      ConfiguredScopes            = 5 [0x00000005]
      UpgradeTime                 = Wed Mar 23 08:52:53 2016 UTC
      User Favorites Path         = file:///C:\Users\DeputyGod\Favorites\
      Version                     = 10.0.10240.16431

Software\Microsoft\Internet Explorer\Privacy not found (IE should use the default
Privacy settings)

Software\Microsoft\Internet Explorer\Recovery
LastWrite Time Wed Mar 23 10:24:32 2016 (UTC)

   Software\Microsoft\Internet Explorer\Recovery\Active
   LastWrite Time Wed Mar 23 10:25:10 2016 (UTC)

   Software\Microsoft\Internet Explorer\Recovery\AdminActive not found.

   Software\Microsoft\Internet Explorer\Recovery\PendingDelete not found.


Software\Microsoft\Internet Explorer\Suggested Sites
LastWrite Time Thu Apr 21 02:49:12 2016 (UTC)
   DataStreamEnabledState        = 1
   DeletePending                 = 0
   IndexID                       = dh»ïÜÑùêgª-£Œ←ØÉ{_Û¨ZÎÿ◀_ê^ÚOF↑B·únY]└∥ö
   IndexID_TIMESTAMP             = µV4îÑ
   LogFileFolder                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\INetCache\Low
   MigrationTime                 = Wed Mar 23 08:52:53 2016 UTC
   UploadDiagInfo                = @    ( ♂                      ã♀  Ljrbxñ  ⌐
HÆjbxÑ HÆjbxÑ  h     h      ∟
   UserID                        =        Ðß  ⊥Ñ◀∎z ÀOÃë    ÷xüÂᴶ`hB·\¬5ã,     ⌐       ╫f
        :»Ë 7ìkX°1GFÑØ9⊓äw4 ·ÚÀÂO‼EÝ     ♫⊓   ⌐      [`·Fqy¾N_D¤InDv^*]êqmÃWà—mÀ@
«¨Îs#!Ç·Fy┤ÛÖíoIXÑþ½Ç|ÚÍÉ⚬ód[È3Åz¢å°@:ðXE↕?,•ZÄÁ÷·Y@&AàÞ⚬EÔ0@
%_®C+«:À'ᴸÉß⌐d44Î7ªO⊡⊡•É~$?.jC¥G,♀÷5 #⚬þ\-ýZß♂Ø¥'nmx
   UserIDGenCode                 = 10
   UserID_TIMESTAMP              = µV4îÑ


-------------------------------------------
internet_settings_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 12 20:55:36 2016 (UTC)
   CertificateRevocation         = true   [1]
   DisableCachingOfSSLPages      = false [0]
   EnableHttp1_1                 = false [0]
```

Page 8

```
                              Admin OUTPUT.txt
    EnableNegotiate            = true   [1]
    IE5_UA_Backup_Flag         = 5.0
    MigrateProxy               = true   [1]
    PrivacyAdvanced            = true   [1]
    ProxyEnable                = false  [0]
    ProxyHttp1.1               = false  [0]
    SecureProtocols            = 2688  [0x00000A80]
    User Agent                 = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    WarnonZoneCrossing         = false  [0]
    ZonesSecurityUpgrade       = Tue Mar 22 13:13:18 2016 UTC


  *Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
  LastWrite Time Tue Mar 22 13:13:21 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
   LastWrite Time Tue Mar 22 13:13:19 2016 (UTC)
     AppContainerContentLimit  = 14885
     AppContainerTotalContentLimit = 14885
     ContentLimit              = 14885
     TotalContentLimit         = 14885
     Version                   = 2


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
   LastWrite Time Tue Mar 22 13:13:22 2016 (UTC)
     CacheLimit                = 256000 KB
     CachePrefix               =


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
   LastWrite Time Tue Mar 22 13:13:18 2016 (UTC)
     CacheLimit                = 1 KB
     CachePrefix               = Cookie:


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
   LastWrite Time Tue Mar 22 13:13:18 2016 (UTC)
     CacheLimit                = 1 KB
     CachePrefix               = Visited:


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache
   LastWrite Time Thu Apr 21 04:31:04 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DNTException
   LastWrite Time Wed Mar 23 10:24:31 2016 (UTC)
     CacheLimit                = 1 KB
     CacheOptions              = 0x300
     CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\INetCookies\DNTException
     CachePrefix               = DNTException:
     CacheRelativePath         = Microsoft\Windows\INetCookies\DNTException
     CacheRepair               = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\DOMStore
   LastWrite Time Wed Mar 23 11:51:57 2016 (UTC)
     CacheLimit                = 1000 KB
     CacheOptions              = 0x8
     CachePath                 = C:\Users\DeputyGod\AppData\Local\Microsoft\Internet
Explorer\DOMStore
     CachePrefix               = DOMStore
     CacheRelativePath         = Microsoft\Internet Explorer\DOMStore
```

Page 9

```
                                    Admin OUTPUT.txt
    CacheRepair                 = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieModeList
    LastWrite Time Wed Mar 23 10:24:38 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 = C:\Users\DeputyGod\AppData\Local\Microsoft\Internet
Explorer\EmieModeList
      CachePrefix               = EmieModeList:
      CacheRelativePath         = Microsoft\Internet Explorer\EmieModeList
      CacheRepair               = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieSiteList
    LastWrite Time Wed Mar 23 10:24:38 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 = C:\Users\DeputyGod\AppData\Local\Microsoft\Internet
Explorer\EmieSiteList
      CachePrefix               = EmieSiteList:
      CacheRelativePath         = Microsoft\Internet Explorer\EmieSiteList
      CacheRepair               = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\EmieUserList
    LastWrite Time Wed Mar 23 10:24:38 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 = C:\Users\DeputyGod\AppData\Local\Microsoft\Internet
Explorer\EmieUserList
      CachePrefix               = EmieUserList:
      CacheRelativePath         = Microsoft\Internet Explorer\EmieUserList
      CacheRepair               = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016032820160404
    LastWrite Time Mon Apr  4 21:50:21 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0xB
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
32820160404
      CachePrefix               = :2016032820160404:
      CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016032820160404
      CacheRepair               = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016040420160411
    LastWrite Time Mon Apr 11 21:48:05 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0xB
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
40420160411
      CachePrefix               = :2016040420160411:
      CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016040420160411
      CacheRepair               = 0x0

  Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016041120160418
                                    Page 10
```

```
                              Admin OUTPUT.txt
    LastWrite Time Mon Apr 18 23:30:31 2016 (UTC)
        CacheLimit                = 1 KB
        CacheOptions              = 0xB
        CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
41120160418
        CachePrefix               = :2016041120160418:
        CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016041120160418
        CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016041820160419
    LastWrite Time Mon Apr 18 23:30:31 2016 (UTC)
        CacheLimit                = 1 KB
        CacheOptions              = 0xB
        CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
41820160419
        CachePrefix               = :2016041820160419:
        CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016041820160419
        CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016041920160420
    LastWrite Time Tue Apr 19 21:25:12 2016 (UTC)
        CacheLimit                = 1 KB
        CacheOptions              = 0xB
        CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
41920160420
        CachePrefix               = :2016041920160420:
        CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016041920160420
        CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016042020160421
    LastWrite Time Wed Apr 20 22:27:35 2016 (UTC)
        CacheLimit                = 1 KB
        CacheOptions              = 0xB
        CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
42020160421
        CachePrefix               = :2016042020160421:
        CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016042020160421
        CacheRepair               = 0x0

    Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016042120160422
    LastWrite Time Thu Apr 21 04:31:04 2016 (UTC)
        CacheLimit                = 1 KB
        CacheOptions              = 0xB
        CachePath                 =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160
42120160422
        CachePrefix               = :2016042120160422:
        CacheRelativePath         =
Microsoft\Windows\History\History.IE5\MSHist012016042120160422
        CacheRepair               = 0x0

                              Page 11
```

Admin OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_DNTException
   LastWrite Time Tue Mar 22 11:10:37 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_D
NTException
      CachePrefix               = MicrosoftEdge_DNTException:
      CacheRelativePath         =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DNTException
      CacheRepair               = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_bingpagedata
   LastWrite Time Tue Mar 22 11:38:02 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_b
ingpagedata
      CachePrefix               = MicrosoftEdge_bingpagedata:
      CacheRelativePath         =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_bingpagedata
      CacheRepair               = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_iecompat
   LastWrite Time Tue Mar 22 11:10:37 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x109
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_i
ecompat
      CachePrefix               = MicrosoftEdge_iecompat:
      CacheRelativePath         =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompat
      CacheRepair               = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_iecompatua
   LastWrite Time Tue Mar 22 11:10:37 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x109
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_i
ecompatua
      CachePrefix               = MicrosoftEdge_iecompatua:
      CacheRelativePath         =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompatua
      CacheRepair               = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_ieflipahead
   LastWrite Time Tue Mar 22 11:38:01 2016 (UTC)
      CacheLimit                = 1 KB
      CacheOptions              = 0x300
      CachePath                 =
C:\Users\DeputyGod\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_i
eflipahead
      CachePrefix               = MicrosoftEdge_ieflipahead:
      CacheRelativePath         =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_ieflipahead
Page 12

```
                                   Admin OUTPUT.txt
     CacheRepair                   = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\feedplat
     LastWrite Time Tue Mar 22 13:13:22 2016 (UTC)
     CacheLimit                    = 1 KB
     CacheOptions                  = 0x0
     CachePath                     = C:\Users\DeputyGod\AppData\Local\Microsoft\Feeds
Cache
     CachePrefix                   = feedplat:
     CacheRelativePath             = Microsoft\Feeds Cache
     CacheRepair                   = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompat
   LastWrite Time Tue Mar 22 13:15:11 2016 (UTC)
     CacheLimit                    = 1 KB
     CacheOptions                  = 0x309
     CachePath                     =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\IECompatCache
     CachePrefix                   = iecompat:
     CacheRelativePath             = Microsoft\Windows\IECompatCache
     CacheRepair                   = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompatua
     LastWrite Time Tue Mar 22 13:15:11 2016 (UTC)
     CacheLimit                    = 1 KB
     CacheOptions                  = 0x309
     CachePath                     =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\IECompatUaCache
     CachePrefix                   = iecompatua:
     CacheRelativePath             = Microsoft\Windows\IECompatUaCache
     CacheRepair                   = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iedownload
     LastWrite Time Wed Mar 23 10:24:32 2016 (UTC)
     CacheLimit                    = 1 KB
     CacheOptions                  = 0x9
     CachePath                     =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\IEDownloadHistory
     CachePrefix                   = iedownload:
     CacheRelativePath             = Microsoft\Windows\IEDownloadHistory
     CacheRepair                   = 0x0



   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
   LastWrite Time Tue Mar 22 11:13:38 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Content
   LastWrite Time Tue Mar 22 11:13:38 2016 (UTC)
     CacheLimit                    = 256000 KB
     CachePrefix                   =

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Cookies
   LastWrite Time Tue Mar 22 11:13:38 2016 (UTC)
     CacheLimit                    = 1 KB
     CachePrefix                   = Cookie:

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\History
   LastWrite Time Tue Mar 22 11:13:38 2016 (UTC)
     CacheLimit                    = 1 KB
                                Page 13
```

```
                              Admin OUTPUT.txt
      CachePrefix                = Visited:


   Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache
   LastWrite Time Wed Mar 23 10:24:37 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\DOMStore
   LastWrite Time Wed Mar 23 10:24:37 2016 (UTC)
      CacheLimit                 = 1000 KB
      CacheOptions               = 0x8
      CachePath                  =
C:\Users\DeputyGod\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore
      CachePrefix                = DOMStore
      CacheRepair                = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\iecompat
   LastWrite Time Wed Mar 23 10:24:33 2016 (UTC)
      CacheLimit                 = 1 KB
      CacheOptions               = 0x309
      CachePath                  =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\IECompatCache\Low
      CachePrefix                = iecompat:
      CacheRelativePath          = Microsoft\Windows\IECompatCache\Low
      CacheRepair                = 0x0

   Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache\iecompatua
   LastWrite Time Wed Mar 23 10:24:33 2016 (UTC)
      CacheLimit                 = 1 KB
      CacheOptions               = 0x309
      CachePath                  =
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\IECompatUaCache\Low
      CachePrefix                = iecompatua:
      CacheRelativePath          = Microsoft\Windows\IECompatUaCache\Low
      CacheRepair                = 0x0


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
   LastWrite Time Tue Mar 22 13:13:02 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History
   LastWrite Time Tue Mar 22 13:13:02 2016 (UTC)
   ANALYST NOTE:
      No per-domain cookie decisions subkeys are present


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
   LastWrite Time Tue Mar 22 13:13:18 2016 (UTC)


 *Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
   LastWrite Time Tue Mar 22 13:13:25 2016 (UTC)
      (default)                  =
      AutoDetect                 = 0
      IntranetName               = 1
      ProxyBypass                = 1
      UNCAsIntranet              = 1
      -- 'ZoneMap' subkeys -- not parsed:
        Domains                     Tue Mar 22 13:13:18 2016 UTC
        ProtocolDefaults            Tue Mar 22 13:13:18 2016 UTC
                              Page 14
```

```
                                    Admin OUTPUT.txt
         Ranges                     Tue Mar 22 13:13:18 2016 UTC

Subkeys not parsed in 'Software\Microsoft\Windows\CurrentVersion\Internet Settings'

        Cache              ---  Tue Mar 22 13:13:02 2016 UTC
        Connections        ---  Thu Apr 21 03:31:50 2016 UTC
        Http Filters       ---  Tue Mar 22 13:13:02 2016 UTC
        Lockdown_Zones     ---  Tue Mar 22 13:13:18 2016 UTC
        Passport           ---  Tue Mar 22 13:13:18 2016 UTC
        Zones              ---  Wed Mar 23 10:24:31 2016 UTC

----------------------------------------
javafx v.20110322
(NTUSER.DAT) Gets contents of user's JavaFX key

Software\JavaSoft\Java Update\Policy\JavaFX not found.
----------------------------------------
listsoft v.20080324
(NTUSER.DAT) Lists contents of user's Software key

listsoft v.20080324
List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

Thu Apr 21 03:27:55 2016Z         Microsoft
Thu Apr 21 03:22:45 2016Z         McAfee
Thu Apr 21 03:17:49 2016Z         McAfeeInstaller
Thu Apr 21 00:00:03 2016Z         Host App Service
Wed Apr 20 22:32:02 2016Z         RegisteredApplications
Tue Apr 12 20:55:04 2016Z         Yahoo
Tue Apr 12 20:48:36 2016Z         Mozilla
Mon Apr  4 21:50:20 2016Z         Macromedia
Thu Mar 24 13:29:21 2016Z         Brother
Thu Mar 24 12:41:59 2016Z         Adobe
Thu Mar 24 11:59:18 2016Z         JavaSoft
Wed Mar 23 10:12:44 2016Z         ForceInterfaceCOM
Wed Mar 23 10:12:08 2016Z         Privax
Tue Mar 22 13:31:25 2016Z         OEM
Tue Mar 22 13:17:41 2016Z         Realtek
Tue Mar 22 13:13:18 2016Z         AppDataLow
Tue Mar 22 13:13:13 2016Z         Local AppWizard-Generated Applications
Tue Mar 22 13:13:08 2016Z         Wow6432Node
Tue Mar 22 13:13:07 2016Z         Intel
Tue Mar 22 13:13:03 2016Z         DashlaneUpgrade
Tue Mar 22 13:13:03 2016Z         Policies
Tue Mar 22 13:13:02 2016Z         Mine
Tue Mar 22 11:49:07 2016Z         Foxit Software
Tue Mar 22 11:49:04 2016Z         Netscape
Tue Mar 22 11:49:04 2016Z         ODBC
Tue Mar 22 10:53:02 2016Z         DataLode
Tue Mar 22 10:45:54 2016Z         Clients
----------------------------------------
liveContactsGUID v.20110221
(NTUSER.DAT) Gets user Windows Live Messenger GUIDs

Software\Microsoft\Windows Live Contacts\Database not found.
----------------------------------------
load v.20100811
(NTUSER.DAT) Gets load and run values from user hive

load
Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Mar 23 09:43:30 2016 (UTC)
                              Page 15
```

Admin OUTPUT.txt

load value not found.
run value not found.
------------------------------------
logonusername v.20080324
(NTUSER.DAT) Get user's Logon User Name value

Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Thu Apr 21 03:21:23 2016 (UTC)]
------------------------------------
mmc v.20080324
(NTUSER.DAT) Get contents of user's MMC\Recent File List key

MMC - Recent File List
Software\Microsoft\Microsoft Management Console\Recent File List
LastWrite Time Tue Mar 29 12:24:26 2016 (UTC)
    File1 -> C:\Windows\system32\devmgmt.msc
------------------------------------
mndmru v.20080324
(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.
------------------------------------
mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Tue Mar 22 13:22:48 2016 (UTC)

Remote Drives:

Volumes:
Tue Mar 22 13:22:48 2016 (UTC)
    {1e043e47-febf-4b10-983a-321680f40f77}
Tue Mar 22 11:05:19 2016 (UTC)
    {33951250-5869-11e5-9bd1-806e6f6e6963}

Drives:
Tue Mar 22 13:13:07 2016 (UTC) - CPC

Unique MAC Addresses:
80:6E:6F:6E:69:63
32:16:80:F4:0F:77

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices
entries that begin with "\??\Volume".
------------------------------------
mpmru v.20080324
(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.
------------------------------------
mspaper v.20080324
(NTUSER.DAT) Gets images listed in user's MSPaper key

SOFTWARE\Microsoft\MSPaper* not found.
------------------------------------
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.
Page 16

Admin OUTPUT.txt

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
------------------------------------------
nero v.20100218
(NTUSER.DAT) Gets contents of Ahead\Nero Recent File List subkeys

Software\Ahead not found.
------------------------------------------
netassist v.20110427
(NTUSER.DAT) Check for Firefox Extensions.

Software\Mozilla\Firefox\Extensions not found.
Software\Microsoft\Windows\CurrentVersion\Uninstall\NetAssistant not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0 not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0\SourceList
not found.


------------------------------------------
odysseus v.20110202
(NTUSER.DAT) Extract registry keys for Odysseus by bindshell.net.

Software\bindshell.net\Odysseus not found.


------------------------------------------
officedocs v.20080324
(NTUSER.DAT) Gets contents of user's Office doc MRU keys

officedocs v.20080324
MSOffice version 12.0 located.



Software\Microsoft\Office\12.0Excel\Recent Files not found.

Software\Microsoft\Office\12.0\PowerPoint\Recent File List not found.
------------------------------------------
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version not found.
------------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

MSOffice version not found.
------------------------------------------
OSVersion
Software\Microsoft
LastWrite Time Thu Apr 21 03:27:55 2016 (UTC)

OSVersion value not found.
------------------------------------------
outlook v.20100218
(NTUSER.DAT) Gets user's Outlook settings

Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
not found.
------------------------------------------
policies_u v.20091021
(NTUSER.DAT) Get values from the user's Policies key


System\EnableProfileQuota value not found.
Page 17

Admin OUTPUT.txt
------------------------------------
printermru v.20091125
(NTUSER.DAT) Gets user's Printer Wizard MRU listing

Printers\Settings\Wizard\ConnectMRU not found.
------------------------------------
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Thu Apr 21 03:21:06 2016

   Microsoft XPS Document Writer (winspool,Ne00:,15,45)
   Microsoft Print to PDF (winspool,Ne01:,15,45)
   Foxit PhantomPDF Printer (winspool,Ne02:,15,45)
   Fax (winspool,Ne03:,15,45)
   Brother MFC-9340CDW USB (winspool,Ne05:,15,45)
   Brother PC-FAX v.3.1 (winspool,Ne04:,15,45)

Default Printer (via CurrentVersion\Windows): Brother MFC-9340CDW USB,winspool,Ne04:
------------------------------------
privoxy v.20110204
(NTUSER.DAT) Extracts the install path for Privoxy.

Software\Privoxy not found.

------------------------------------
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Tue Apr 12 20:55:36 2016 (UTC)
   CertificateRevocation        1
   DisableCachingOfSSLPages     0
   EnableHttp1_1                0
   EnableNegotiate              1
   IE5_UA_Backup_Flag           5.0
   MigrateProxy                 1
   PrivacyAdvanced              1
   ProxyEnable                  0
   ProxyHttp1.1                 0
   SecureProtocols              2688
   User Agent                   Mozilla/4.0 (compatible; MSIE 8.0; Win32)
   WarnonZoneCrossing           0
   ZonesSecurityUpgrade         2586292023
------------------------------------
publishingwizard v.20110202
(NTUSER.DAT) Extract AddNetPlace\LocationMRU for Microsoft Publishing Wizard

Software\Microsoft\Windows\CurrentVersion\Explorer\PublishingWizard\AddNetworkPlace\
AddNetPlace\LocationMRU not found.

------------------------------------
putty v.20110204
(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.

------------------------------------
rdphint v.20090715
(NTUSER) Gets hosts logged onto via RDP and the Domain\Username

Page 18

Admin OUTPUT.txt
Software\Microsoft\Terminal Server Client\Servers not found.
-----------------------------------------
realplayer6 v.20080324
(NTUSER.DAT) Gets user's RealPlayer v6 MostRecentClips(Default) values

Software\RealNetworks\RealPlayer\6.0\Preferences not found.
-----------------------------------------
realvnc v.20091125
(NTUSER.DAT) Gets user's RealVNC MRU listing

Software\RealVNC\VNCViewer4\MRU not found.
-----------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Thu Apr 21 04:39:41 2016 (UTC)
  21 = New folder (7)
  84 = 11611301081%20(18).jpg
  43 = 80011301081%20(7).jpg
  38 = New folder (2)
  89 = selfie 23.jpg
  0 = CheerLeader
  88 = CheerLeader
  94 = Delete
  3 = The Internet
  96 = Julia Stockholm
  63 = Uninstall
  14 = Downloads
  95 = Nancy Arlington VA
  28 = New folder
  81 = Janet VA 34 bimom
  18 = Michelle Bethlehem
  64 = 18.jpg
  93 = 19.jpg
  80 = 3.mp4
  79 = 8.jpg
  77 = 119.jpg
  74 = 118.jpg
  72 = 26.jpg
  69 = 114.jpg
  67 = 51.jpg
  70 = 28.jpg
  44 = 152.jpg
  52 = 150.jpg
  66 = 113.jpg
  51 = 32.jpg
  49 = 112.jpg
  48 = 121.jpg
  92 = 151.jpg
  42 = Yahoo!
  41 = YUpdater
  91 = Bathing Suit
  90 = Heels
  87 = Lady
  86 = Sara16 CO
  85 = Megan Fredericksburg
  45 = Pregnant & milk
  83 = 87301301081%20(14).jpg
  82 = Beverly NJ
  65 = New folder (11)

Page 19

Admin OUTPUT.txt

```
53 = Cock
20 = Harini
25 = Attachments_201647.zip
62 = FB
29 = New folder (4)
19 = Danna CA
78 = Documents
76 = Sara NY
75 = 35
22 = Dave
73 = 32
71 = 23
68 = Lyana PalmBeachFL
47 = Tina Erin
2 = dateandtime
61 = windowsupdate
60 = Changing MAC.docx
5 = All Tasks
59 = {BD256B65-94BE-4194-84BF-41D50D0EF26E}
58 = {55EA023B-F961-4C4B-8D92-4F109156466E}
55 = {88C9D04D-39DD-41EE-A63B-23218D69717F}
57 = {EDB046FF-3554-4BD0-B152-DE4DF7071CA8}
56 = Network and Internet
54 = Matilynn
31 = Amanda
50 = New folder (8)
46 = Hillary
7 = System and Security
6 = ::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE}
24 = Jack
40 = New folder (10)
37 = New folder (9)
39 = piercings
35 = New folder (6)
34 = New folder (5)
32 = mooning
33 = Beach
30 = New folder (3)
27 = Jasmine
26 = Billy
23 = This PC
17 = User Accounts
16 = ::{60632754-C523-4B62-B45C-4172DA012619}
13 = Program Files (x86)
12 = Mozilla Firefox
15 = DeputyGod
11 = ms-windows-store:///
10 =
news?FORM=WNSPN1&q=top+stories&ts=1458647420401&nclid=BBA8597EFC3EAB89896A78DCF68F77
63
9 = Templates
8 = Normal.dotm
4 = {D58D0F32-9128-40D3-89AF-8C63C5167C99}
1 = DVD RW Drive (E:) OFFICE12

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.0&affid=662&hres=1366
&vres=768&LaunchPoint=19&pkgs=431_662_en-us_1_354FA342-AB76-41A7
LastWrite Time Thu Apr 21 02:53:13 2016 (UTC)
MRUListEX =

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.1043&x-mid=IP-chartTe
st-09
LastWrite Time Sun Mar 27 08:58:55 2016 (UTC)
```

Page 20

Admin OUTPUT.txt

MRUListEx =

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time Tue Mar 29 12:24:54 2016 (UTC)
MRUListEx = 0
  0 = Changing MAC.docx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.dotm
LastWrite Time Tue Mar 22 11:49:56 2016 (UTC)
MRUListEx = 0
  0 = Normal.dotm

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.inf
LastWrite Time Tue Mar 22 13:23:02 2016 (UTC)
MRUListEx = 0
  0 = autorun.inf

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
LastWrite Time Thu Apr 21 04:39:41 2016 (UTC)
MRUListEx = 12,4,5,3,2,1,0,19,18,17,16,13,14,6,11,15,10,9,8,7
  12 = 11611301081%20(18).jpg
  4 = 80011301081%20(7).jpg
  5 = selfie 23.jpg
  3 = 18.jpg
  2 = 19.jpg
  1 = 8.jpg
  0 = 119.jpg
  19 = 118.jpg
  18 = 26.jpg
  17 = 114.jpg
  16 = 51.jpg
  13 = 28.jpg
  14 = 152.jpg
  6 = 150.jpg
  11 = 113.jpg
  15 = 32.jpg
  10 = 112.jpg
  9 = 121.jpg
  8 = 151.jpg
  7 = 87301301081%20(14).jpg

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mp4
LastWrite Time Tue Apr 12 22:10:57 2016 (UTC)
MRUListEx = 0
  0 = 3.mp4

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip
LastWrite Time Thu Apr  7 15:41:10 2016 (UTC)
MRUListEx = 0
  0 = Attachments_201647.zip

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Thu Apr 21 04:39:41 2016 (UTC)
MRUListEx =
25,23,27,11,1,10,8,26,20,12,18,24,22,21,19,14,17,2,16,15,3,13,9,7,5,6,4,0
  25 = New folder (7)
  23 = New folder (2)
  27 = Fashion
  11 = Delete
  1 = The Internet
  10 = Uninstall
  8 = Downloads
  26 = New folder

Page 21

Admin OUTPUT.txt
```
20 = Michelle Bethlehem
12 = Yahoo!
18 = Cock
24 = Harini
22 = FB
21 = New folder (4)
19 = Documents
14 = Dave
17 = Tina Erin
2 = All Tasks
16 = Network and Internet
15 = New folder (8)
3 = System and Security
13 = Jack
9 = This PC
7 = User Accounts
5 = Program Files (x86)
6 = DeputyGod
4 = Templates
0 = DVD RW Drive (E:) OFFICE12
```

------------------------------------
rootkit_revealer v.20110204
(NTUSER.DAT) Extracts the EULA value for Sysinternals Rootkit Revealer.

Software\Sysinternals\RootkitRevealer not found.

------------------------------------
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Tue Mar 22 12:50:12 2016 (UTC)
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU has no values.
------------------------------------
Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
------------------------------------
shellfolders v.20090115
(NTUSER.DAT) Retrieve user Shell Folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
LastWrite Time Tue Mar 22 13:13:25 2016 (UTC)
!Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath
function instead
AppData               C:\Users\DeputyGod\AppData\Roaming
Local AppData         C:\Users\DeputyGod\AppData\Local
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Libraries
My Video              C:\Users\DeputyGod\Videos
My Pictures           C:\Users\DeputyGod\Pictures
Desktop               C:\Users\DeputyGod\Desktop
History               C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\History
NetHood               C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Network
Shortcuts
{56784854-C6CB-462B-8169-88E350ACB882} C:\Users\DeputyGod\Contacts
{00BCFC5A-ED94-4E48-96A1-3F6217F21990}
C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\RoamingTiles
Cookies               C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\INetCookies
Favorites             C:\Users\DeputyGod\Favorites
SendTo                C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu            C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Start Menu
```
Page 22

```
                              Admin OUTPUT.txt
My Music                 C:\Users\DeputyGod\Music
Programs                 C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs
Recent                   C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Recent
CD Burning               C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\Burn\Burn
PrintHood                C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Printer
Shortcuts
{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\DeputyGod\Searches
{374DE290-123F-4565-9164-39C4925E467B} C:\Users\DeputyGod\Downloads
{A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\DeputyGod\AppData\LocalLow
Startup                  C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Administrative Tools C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
Personal                 C:\Users\DeputyGod\Documents
{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\DeputyGod\Links
Cache                    C:\Users\DeputyGod\AppData\Local\Microsoft\Windows\INetCache
Templates                C:\Users\DeputyGod\AppData\Roaming\Microsoft\Windows\Templates
{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\DeputyGod\Saved Games
Fonts                    C:\Windows\Fonts


----------------------------------------
Software\Skype not found.
----------------------------------------
snapshot_viewer v.20110210
(NTUSER.DAT) Extracts Recent File List for Microsoft Snapshot Viewer.

Software\Microsoft\Snapshot Viewer\Recent File List not found.


----------------------------------------
ssh_host_keys v.20120809
(NTUSER.DAT) Extracts Putty/WinSCP SSH Host Keys

"Software\SimonTatham\Putty\SshHostKeys" does not exist

"Software\Martin Prikryl\WinSCP 2\SshHostKeys" does not exist
----------------------------------------
startmenuinternetapps_cu v.20101219
(NTUSER.DAT) Start Menu Internet Applications info current user

Start-Menu Internet Applications

StartMenuInternet [Tue Mar 22 10:45:54 2016 (UTC)]
NOTE: default Internet Browser client key
(default) -> FIREFOX.EXE


----------------------------------------
startpage v.20100330
(NTUSER.DAT) Gets contents of user's StartPage key

Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage
LastWrite Time Tue Mar 22 13:14:44 2016 (UTC)

StartMenu_Start_Time    = Tue Mar 22 13:13:07 2016 Z
----------------------------------------
streammru v.20090205
(NTUSER.DAT) streammru

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
----------------------------------------
streams v.20081124
(NTUSER.DAT) Parse Streams and StreamsMRU entries
```

Page 23

Admin OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
------------------------------------------
Software\SysInternals not found.
------------------------------------------
trustrecords v.20120716
Word

PowerPoint

Excel

Access

------------------------------------------
Launching tsclient v.20120827
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
------------------------------------------
typedpaths v.20100330
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
LastWrite Time Tue Mar 22 12:50:12 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
------------------------------------------
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Tue Mar 22 13:13:21 2016 (UTC)
  url1 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
------------------------------------------
typedurlstime v.20120613
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

Software\Microsoft\Internet Explorer\TypedURLsTime not found.
------------------------------------------
unreadmail v.20100218
(NTUSER.DAT) Gets contents of Unreadmail key

Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
------------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Fri Apr 15 18:24:39 2016 (UTC)
  20090604: C:\Program Files (x86)\Encore\Hoyle Puzzle and Board Games
2011\Ereg\encore_reg.exe /r "C:\Program Files (x86)\Encore\Hoyle Puzzle and Board
Games 2011\Ereg\encore_reg.rpd"
  AcerPortal: "C:\Program Files (x86)\Acer\Acer Portal\AcerPortal.exe" startup


  OneDrive: "C:\Users\DeputyGod\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
/background

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Page 24

Admin OUTPUT.txt

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Thu Apr 21 03:05:50 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.


Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Mar 23 09:43:30 2016 (UTC)
Run value not found.
run value not found.
load value not found.
------------------------------------
user_win v.20080415
(NTUSER.DAT)  --

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Wed Mar 23 09:43:30 2016 (UTC)

------------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Mar 22 13:13:21 2016 (UTC)

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Thu Apr 21 04:24:45 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Encore\Hoyle Puzzle and Board Games
2011\Hoyle Puzzle Games.exe (12)
Thu Apr 21 03:31:46 2016 Z
  E7CF176E110C211B (51)
Thu Apr 21 03:29:08 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\HMA! Pro VPN\bin\HMA! Pro VPN.exe (16)
Thu Apr 21 03:24:55 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Yahoo!\Messenger\YahooMessenger.exe (22)
Thu Apr 21 02:53:13 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Mozilla Firefox\firefox.exe (1)
Wed Apr 20 02:09:30 2016 Z
  Microsoft.Windows.Explorer (10)

Page 25

Admin OUTPUT.txt

Tue Apr 12 20:54:59 2016 Z
  C:\Users\DeputyGod\Downloads\msgr11us.exe (1)
Tue Apr 12 20:52:21 2016 Z
  Microsoft.Windows.ControlPanel (7)
Tue Apr 12 20:47:33 2016 Z

windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
(1)
Thu Apr  7 20:34:55 2016 Z
  Malwarebytes.ToastNotification (0)
Sat Apr  2 03:47:09 2016 Z
  Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge (0)
Sat Apr  2 03:35:30 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Adobe\Photoshop Elements
2\PhotoshopElements.exe (0)
Tue Mar 29 12:25:18 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (0)
Tue Mar 29 12:24:29 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft office\Office12\WINWORD.EXE (0)
Tue Mar 29 12:18:42 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mmc.exe (0)
Tue Mar 29 12:15:36 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (0)
Tue Mar 29 09:28:41 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe (0)
Sun Mar 27 13:04:53 2016 Z
  C:\Users\DeputyGod\Downloads\mbae-setup-1.08.1.1189.exe (0)
Fri Mar 25 15:16:25 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\sfc.exe (0)
Thu Mar 24 13:28:56 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Brother\BrLauncher\BrLauncher.exe (0)
Tue Mar 22 13:23:19 2016 Z
  E:\setup.exe (0)
Tue Mar 22 13:23:02 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (0)
Tue Mar 22 13:12:57 2016 Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (0)
  Microsoft.SkypeApp_kzf8qxf38zg5c!App (0)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (0)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (0)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (0)
  Microsoft.WindowsAlarms_8wekyb3d8bbwe!App (0)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (0)
  Microsoft.Windows.StickyNotes (0)
Tue Mar 22 13:11:18 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SystemPropertiesProtection.exe (0)
Tue Mar 22 11:51:40 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft office\Office12\POWERPNT.EXE (0)
Tue Mar 22 11:50:41 2016 Z
  Microsoft.AutoGenerated.{F68CDADD-FCBB-CBB5-6BC6-07D9FB3DA1A3} (0)
Tue Mar 22 11:44:20 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\systemreset.exe (0)
Tue Mar 22 11:39:23 2016 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SystemPropertiesComputerName.exe (0)
Tue Mar 22 10:58:40 2016 Z
  E:\AutoPlay.exe (0)
Tue Mar 22 10:54:24 2016 Z
  McAfee.McAgent (0)
Tue Mar 22 10:48:01 2016 Z
  E:\HoylePuzzleGames2011.exe (0)

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}

Page 26

Admin OUTPUT.txt
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Thu Apr 21 04:24:45 2016 Z
   C:\Users\Public\Desktop\Hoyle Puzzle and Board Games 2011.lnk (12)
Thu Apr 21 03:31:46 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Mozilla Firefox.lnk (33)
Thu Apr 21 03:29:08 2016 Z
   C:\Users\Public\Desktop\HMA! Pro VPN.lnk (16)
Thu Apr 21 03:24:55 2016 Z
   C:\Users\Public\Desktop\Yahoo! Messenger.lnk (22)
Thu Apr 21 02:49:23 2016 Z
   C:\Users\DeputyGod\Desktop\Mozilla Firefox.lnk (18)
Wed Apr 20 02:09:30 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk (10)
Tue Apr 12 20:52:21 2016 Z
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Control Panel.lnk (4)
Thu Apr  7 20:34:55 2016 Z
   C:\Users\Public\Desktop\Malwarebytes Anti-Malware.lnk (0)
Sat Apr  2 03:35:30 2016 Z
   C:\Users\Public\Desktop\Adobe Photoshop Elements 2.0.lnk (0)
Tue Mar 29 12:25:18 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (0)
Tue Mar 29 12:24:29 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office\Microsoft Office Word
2007.lnk (0)
   C:\Users\DeputyGod\Desktop\Microsoft Office Word 2007.lnk (0)
Tue Mar 29 12:15:36 2016 Z
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk (0)
Sun Mar 27 12:05:34 2016 Z
   C:\Users\DeputyGod\Desktop\Snipping Tool.lnk (0)
Sun Mar 27 08:25:35 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Mozilla Firefox.lnk (0)
Thu Mar 24 13:28:56 2016 Z
   C:\Users\Public\Desktop\Brother Utilities.lnk (0)
Tue Mar 22 13:12:57 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (0)
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk (0)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (0)
Tue Mar 22 11:51:40 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office\Microsoft Office
PowerPoint 2007.lnk (0)
Tue Mar 22 11:50:41 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office.lnk (0)
Tue Mar 22 10:54:24 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\McAfee\McAfee LiveSafe - Internet
Security.lnk (0)

{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}

----------------------------------------
userinfo v.20130513
(NTUSER.DAT) Gets contents of MS Office UserInfo values

Software\Microsoft\Office\Common\UserName = Unknown

Software\Microsoft\Office\Common\UserInfo
LastWrite Time Tue Mar 22 11:49:07 2016 (UTC)
   UserName         DeputyGod
   Company
   UserInitials    D

Software\Microsoft\Office\11\.0\Common\UserInfo not found.

----------------------------------------
                        Page 27

Admin OUTPUT.txt

userlocsvc v.20090411
(NTUSER.DAT) Displays contents of User Location Service\Client key

Software\Microsoft\User Location Service\Client not found.
------------------------------------------
vista_bitbucket v.20080420
(NTUSER.DAT) Get BitBucket settings from Vista via NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Tue Mar 22 13:17:31 2016 (UTC)

LastEnum : 0,{1e043e47-febf-4b10-983a-321680f40f77}

{1e043e47-febf-4b10-983a-321680f40f77} [Sat Apr  9 00:59:04 2016] (UTC)
    NukeOnDelete      0
------------------------------------------
vmplayer v.20110204
(NTUSER.DAT) Extracts full filepath for recent VMware Player VM images.

Software\VMware, Inc.\VMware Player\VMplayer\Window position not found.

------------------------------------------
vmware_vsphere_client v.20110204
(NTUSER.DAT) Extract recent connections list for VMware vSphere Client.

Software\VMware\Virtual Infrastructure Client\Preferences\UI\ClientsXml not found.
Software\VMware\VMware Infrastructure Client\Preferences not found.

------------------------------------------
vnchookapplicationprefs v.20110208
(NTUSER.DAT) Get VNCHooks Application Prefs list

Software\ORL\VNCHooks\Application_Prefs not found.
------------------------------------------
vncviewer v.20121231
(NTUSER.DAT) Get VNCViewer system list

Software\ORL\VNCviewer\MRU not found.
Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------------
wallpaper v.200800810
(NTUSER.DAT) Parses Wallpaper MRU Entries

Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper\MRU not found.
------------------------------------------
warcraft3 v.20110202
(NTUSER.DAT) Extract usernames for Warcraft 3.

Software\Blizzard Entertainment\Warcraft III\String not found.

------------------------------------------
winlivemail v.20111118
(NTUSER.DAT) Get & display the contents of the Windows Live Mail key

Software\Microsoft\Windows Live Mail not found.
------------------------------------------
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Apr 21 04:41:01 2016 (UTC)
    FirstLogon = 0
    ParseAutoexec = 1

Page 28

Admin OUTPUT.txt

```
  BuildNumber = 10240
  ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin;OneDrive;Work
Folders
  PUUActive = b5 a7 bd 5a 02 00 04 00 3b 00 a6 00 83 71 06 00 00 83 06 00 c7 39 0d
00 d0 00 00 00 16 00 36 00 06 d2 51 5d 7b b5 1f 00 8b 80 09 00 cf d4 03 00 a2 6b 02
00 3f 2e 01 00 74 c9 02 00 15 57 09 00 e7 1d 00 00 e6 00 00 00 5b db 75 01 88 9b d1
01
```

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
   system had been infected with Bredolab (Symantec).  Also, check the
   contents of a "shell" value - should only include Explorer.exe, if
   it exists.
-----------------------------------------
winrar v.20080819
(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.
-----------------------------------------
winscp_sessions v.20120809
(NTUSER.DAT) Extracts WinSCP stored session data

"Software\Martin Prikryl\WinSCP 2\Sessions" does not exist
-----------------------------------------
winvnc v.20110202
(NTUSER.DAT) Extracts the encrypted password for WinVNC.

Software\ORL\WinVNC3 not found.
Software\ORL\WinVNC3\Default not found.
Software\ORL\WinVNC\Default not found.
Software\RealVNC\WinVNC4 not found.
Software\RealVNC\Default not found.


-----------------------------------------
winzip v.20140730
(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.
-----------------------------------------
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Fri Mar 25 15:13:56 2016 (UTC)

Searches listed in MRUListEx order

5     retail*
4     retaildemo
3     retail demo
2     .tmp
1     amazon
0     .json
-----------------------------------------
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

LastWrite Time Tue Apr 19 21:25:07 2016 (UTC) pager
   Version            = 11.5.0.0228
   Launch on Startup  = 0
   Connection Server  =
   Last Login UserName =
   Last Local IP      =

Page 29

Admin OUTPUT.txt

```
AutoLogin              = 0
Save Password          = 0
Encrypted Password  =
Yahoo Token         =
NOTE: you should not be able to obtain the password.

LastWrite Time Thu Apr 21 03:25:30 2016 (UTC) profiles
Found 1 users.
Found 0 bad users logins.

USER: callme_tim
LastWrite Time Thu Apr 21 04:40:57 2016 (UTC) callme_tim
pref = General
    LastWrite Time Tue Apr 12 20:57:39 2016 (UTC) Alerts
    Missing expected value 'Total Login Tries'
    Missing expected value 'Total Disconnects'
    LastWrite Time Tue Apr 12 20:57:39 2016 (UTC) Archive
    Missing expected value 'Enabled'
    Missing expected value 'Autodelete'
    NOTE: cannot determine archived messages policy due to missing values.
    Missing expected value 'CallHistoryEnabled'
    Missing expected value 'CallHistoryAutodelete'
    NOTE: cannot determine call history policy due to missing values.
    Missing expected 'FriendIcons' subkey.
    Missing expected 'FT' subkey.

------------------------------------------------
ALERT: user_run: Odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup
```

Page 30

Admin2 OUTPUT.txt

acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
------------------------------------------
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
------------------------------------------
aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install

Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
------------------------------------------
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.

Software\SmartLine Vision\aports not found.

------------------------------------------
appcompatflags v.20130930
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.


Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Store
    Fri Jul 10 10:59:56 2015 - C:\Program Files\Acer\Acer Quick Access\QAAgent.exe
    Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbam.exe
    Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\Mozilla Firefox\firefox.exe
    Fri Jul 10 11:00:24 2015 -
C:\Users\Mallik\AppData\Local\Microsoft\OneDrive\17.3.5892.0626\FileSyncConfig.exe
    Fri Jul 10 11:00:24 2015 -
C:\Users\Mallik\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
    Fri Jul 10 11:00:24 2015 -
C:\Users\Mallik\AppData\Local\Microsoft\OneDrive\17.3.6302.0225\FileSyncConfig.exe
    Fri Jul 10 11:00:24 2015 - C:\Program Files
(x86)\Yahoo!\Messenger\YahooMessenger.exe
    Fri Jul 10 11:00:24 2015 -
C:\Users\Mallik\AppData\Local\Temp\jre-8u77-windows-au.exe
    Fri Jul 10 11:00:24 2015 - C:\Program Files (x86)\HMA! Pro VPN\bin\HMA! Pro
VPN.exe
------------------------------------------
applets v.20140723
(NTUSER.DAT) Gets contents of user's Applets key

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Fri Mar 25 10:57:42 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
------------------------------------------
Software\Microsoft\IntelliPoint\AppSpecific not found.
------------------------------------------
Software\Ares not found.
------------------------------------------
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
------------------------------------------
Page 1

Admin2 OUTPUT.txt

autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task

Control Panel\Desktop

AutoEndTasks value not found.
----------------------------------------
autorun v.20081212
(NTUSER.DAT) Gets autorun settings

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer not found.
----------------------------------------
bitbucket_user v.20091020
(NTUSER.DAT) TEST - Get user BitBucket values

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Fri Mar 25 10:57:43 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume
LastWrite Time = Fri Mar 25 10:55:21 2016 (UTC)

----------------------------------------
brisv v.20130429
(NTUSER.DAT) Detect artifacts of a Troj.Brisv.A infection

Software\Microsoft\PIMSRV not found.
----------------------------------------
cain v.20110204
(NTUSER.DAT) Extracts details for Cain & Abel by oxid.it

Software\Cain\Settings not found.

----------------------------------------
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.

----------------------------------------
clampi v.20091019
(NTUSER.DAT) TEST - Checks for keys set by Trojan.Clampi PROT module

Software\Microsoft\Internet Explorer\Main
LastWrite Time Fri Mar 25 11:19:30 2016 (UTC)


Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete not found.

Software\Microsoft\Internet Account Manager\Accounts not found.

The system does not appear to have been infected with the Trojan.Clampi
PROT module.
----------------------------------------
clampitm v.20100624
(NTUSER.DAT) Checks for IOCs for Clampi (per Trend Micro)

ClampiTM plugin
Software\Microsoft\Internet Explorer\Settings
LastWrite Time Fri Mar 25 10:52:04 2016 (UTC)

No Clampi values found.
----------------------------------------
comdlg32 v.20121008

Page 2

Admin2 OUTPUT.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time Fri Mar 25 11:11:02 2016 (UTC)
CIDSizeMRU
LastWrite: Fri Mar 25 11:26:30 2016
Note: All value names are listed in MRUListEx order.

   firefox.exe

LastVisitedPidlMRU
LastWrite: Fri Mar 25 11:11:40 2016
Note: All value names are listed in MRUListEx order.

   firefox.exe - My Computer\C:\.\.

----------------------------------------
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Persisted not found.
----------------------------------------
compdesc v.20080324
(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions not found.
----------------------------------------
controlpanel v.20080428
(NTUSER.DAT) Look for RecentTask* values in ControlPanel key (Vista)

Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel not found.
----------------------------------------
cpldontload v.20100116
(NTUSER.DAT) Gets contents of user's Control Panel don't load key

Control Panel\don't load
LastWrite Time Fri Mar 25 10:57:57 2016 (UTC)

Control Panel\don't load has no values.
----------------------------------------
decaf v.20110210
(NTUSER.DAT) Extracts the EULA value for DECAF.

Software\DECAFme not found.


----------------------------------------
dependency_walker v.20110204
(NTUSER.DAT) Extracts Recent File List for Dependency Walker.

Software\Microsoft\Dependency Walker\Recent File List not found.


----------------------------------------
domains v.20100116
(NTUSER.DAT) Gets contents Internet Settings\ZoneMap\Domains key

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
LastWrite Time Fri Mar 25 10:52:40 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap has no subkeys.
----------------------------------------
environment v.20110204
(NTUSER.DAT) Extracts user's Environment paths from NTUSER.DAT

Environment
Environment
LastWrite Time Fri Mar 25 10:52:04 2016 (UTC)

Page 3

Admin2 OUTPUT.txt

```
TEMP -> %USERPROFILE%\AppData\Local\Temp
TMP -> %USERPROFILE%\AppData\Local\Temp

----------------------------------------
fileexts v.20080818
(NTUSER.DAT) Get user FileExts values

fileexts
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

----------------------------------------
filehistory v.20120620
(NTUSER.DAT) Gets filehistory settings

Software\Microsoft\Windows\CurrentVersion\FileHistory
LastWrite Time Fri Mar 25 10:52:04 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\FileHistory has no values.
File History may not be configured for this user.
----------------------------------------
gthist v.20100218
(NTUSER.DAT) Gets Google Toolbar Search History

Software\Google\NavClient\1.1\History not found.
----------------------------------------
gtwhitelist v.20100218
(NTUSER.DAT) Gets Google Toolbar whitelist values

Software\Google\Google Toolbar\4.0\whitelist not found.
----------------------------------------
haven_and_hearth v.20110204
(NTUSER.DAT) Extracts the username and savedtoken for Haven & Hearth.

Software\JavaSoft\Prefs\haven not found.

----------------------------------------
ie_settings v.20130731
(NTUSER.DAT) Gets important user IE settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Fri Mar 25 10:55:06 2016 (UTC)

User Agent = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade = Wed Mar 23 08:52:53 2016 (UTC)
DaysToKeep value not found - default is 20 days
----------------------------------------
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Fri Mar 25 10:54:48 2016 (UTC)
   Download Directory = ''

Software\Microsoft\Internet Explorer\AutoComplete not found.

Software\Microsoft\Internet Explorer\DOMStorage not found.

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Fri Mar 25 10:52:39 2016 (UTC)
   Internet Explorer version = 0.0.0.0

Software\Microsoft\Internet Explorer\Main
```

Page 4

Admin2 OUTPUT.txt

```
LastWrite Time Fri Mar 25 11:19:30 2016 (UTC)
    Anchor Underline                        = yes
    ApplicationTileImmersiveActivation      = 0
    AssociationActivationMode               = 2
    Cache_Update_Frequency                  = yes
    Default_Page_URL                        = http://acer15.msn.com/?pc=ACTE
    Disable Script Debugger                 = yes
    DisableFirstRunCustomize                = 1
    DisableScriptDebuggerIE                 = yes
    Display Inline Images                   = yes
    Do404Search                             = 1 [0x01000000]
    EdgeSwitchingOSBuildNumber              = 10240.th1_st1.160222-1812
    Enable Browser Extensions               = yes
    ImageStoreRandomFolder                  = q0sw0h9
    Local Page                              = %11%\blank.htm
    OperationalData                         =
    Play_Animations                         = yes
    Play_Background_Sounds                  = yes
    Save_Session_History_On_Exit            = no
    Search Page                             =
http://go.microsoft.com/fwlink/?LinkId=54896
    Show_FullURL                            = no
    Show_StatusBar                          = yes
    Show_ToolBar                            = yes
    Show_URLToolBar                         = yes
    Show_URLinStatusBar                     = yes
    Start Page                              = http://acer15.msn.com/?pc=ACTE
    UseClearType                            = no
    Use_DlgBox_Colors                       = yes
    XMLHTTP                                 = true  [1]
    Software\Microsoft\Internet Explorer\Main\WindowsSearch not found.

Software\Microsoft\Internet Explorer\Privacy not found (IE should use the default
Privacy settings)

Software\Microsoft\Internet Explorer\Recovery not found.

Software\Microsoft\Internet Explorer\Suggested Sites
LastWrite Time Fri Mar 25 10:52:29 2016 (UTC)
    LogFileFolder                           =
C:\Users\Mallik\AppData\Local\Microsoft\Windows\INetCache\Low


-------------------------------------------------
internet_settings_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Fri Mar 25 10:55:06 2016 (UTC)
    CertificateRevocation                   = true   [1]
    DisableCachingOfSSLPages                = false  [0]
    EnableNegotiate                         = true   [1]
    IE5_UA_Backup_Flag                      = 5.0
    MigrateProxy                            = true   [1]
    PrivacyAdvanced                         = true   [1]
    ProxyEnable                             = false  [0]
    SecureProtocols                         = 2688 [0x00000A80]
    User Agent                              = Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    WarnonZoneCrossing                      = false [0]
    ZonesSecurityUpgrade                    = Wed Mar 23 08:52:53 2016 UTC


  *Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
    LastWrite Time Fri Mar 25 10:52:40 2016 (UTC)
```
Page 5

Admin2 OUTPUT.txt

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
LastWrite Time Fri Mar 25 10:52:35 2016 (UTC)
    AppContainerContentLimit   = 14885
    AppContainerTotalContentLimit = 14885
    ContentLimit               = 14885
    TotalContentLimit          = 14885
    Version                    = 2

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
LastWrite Time Fri Mar 25 10:52:41 2016 (UTC)
    CacheLimit                 = 256000 KB
    CachePrefix                =

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
LastWrite Time Fri Mar 25 10:52:35 2016 (UTC)
    CacheLimit                 = 1 KB
    CachePrefix                = Cookie:

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
LastWrite Time Fri Mar 25 10:52:35 2016 (UTC)
    CacheLimit                 = 1 KB
    CachePrefix                = Visited:


Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache
    LastWrite Time Fri Mar 25 11:21:17 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MSHist012016032520160326
    LastWrite Time Fri Mar 25 10:54:24 2016 (UTC)
    CacheLimit                 = 1 KB
    CacheOptions               = 0xB
    CachePath                  =
C:\Users\Mallik\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist0120160325
20160326
    CachePrefix                = :2016032520160326:
    CacheRelativePath          =
Microsoft\Windows\History\History.IE5\MSHist012016032520160326
    CacheRepair                = 0x0

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_DNTException
    LastWrite Time Fri Mar 25 11:21:17 2016 (UTC)
    CacheLimit                 = 1 KB
    CacheOptions               = 0x300
    CachePath                  =
C:\Users\Mallik\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DNTE
xception
    CachePrefix                = MicrosoftEdge_DNTException:
    CacheRelativePath          =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DNTException
    CacheRepair                = 0x0

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_iecompat
    LastWrite Time Fri Mar 25 11:21:16 2016 (UTC)
    CacheLimit                 = 1 KB
    CacheOptions               = 0x109
    CachePath                  =
C:\Users\Mallik\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_ieco
mpat
                            Page 6

```
                                    Admin2 OUTPUT.txt
      CachePrefix              = MicrosoftEdge_iecompat:
      CacheRelativePath        =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompat
      CacheRepair              = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\MicrosoftEdge_iecompatua
   LastWrite Time Fri Mar 25 11:21:17 2016 (UTC)
      CacheLimit               = 1 KB
      CacheOptions             = 0x109
      CachePath                =
C:\Users\Mallik\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_ieco
mpatua
      CachePrefix              = MicrosoftEdge_iecompatua:
      CacheRelativePath        =
MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompatua
      CacheRepair              = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\feedplat
   LastWrite Time Fri Mar 25 10:52:41 2016 (UTC)
      CacheLimit               = 1 KB
      CacheOptions             = 0x0
      CachePath                = C:\Users\Mallik\AppData\Local\Microsoft\Feeds Cache
      CachePrefix              = feedplat:
      CacheRelativePath        = Microsoft\Feeds Cache
      CacheRepair              = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompat
   LastWrite Time Fri Mar 25 10:54:21 2016 (UTC)
      CacheLimit               = 1 KB
      CacheOptions             = 0x309
      CachePath                =
C:\Users\Mallik\AppData\Local\Microsoft\Windows\IECompatCache
      CachePrefix              = iecompat:
      CacheRelativePath        = Microsoft\Windows\IECompatCache
      CacheRepair              = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible
Cache\iecompatua
   LastWrite Time Fri Mar 25 10:54:21 2016 (UTC)
      CacheLimit               = 1 KB
      CacheOptions             = 0x309
      CachePath                =
C:\Users\Mallik\AppData\Local\Microsoft\Windows\IECompatUaCache
      CachePrefix              = iecompatua:
      CacheRelativePath        = Microsoft\Windows\IECompatUaCache
      CacheRepair              = 0x0


   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
   LastWrite Time Fri Mar 25 11:15:50 2016 (UTC)

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Content
   LastWrite Time Fri Mar 25 11:15:50 2016 (UTC)
      CacheLimit               = 256000 KB
      CachePrefix              =

   Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Cookies
   LastWrite Time Fri Mar 25 11:15:50 2016 (UTC)
      CacheLimit               = 1 KB
      CachePrefix              = Cookie:
```

Page 7

Admin2 OUTPUT.txt

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\History
LastWrite Time Fri Mar 25 11:15:50 2016 (UTC)
    CacheLimit                      = 1 KB
    CachePrefix                     = Visited:


Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\LowCache\Extensible Cache
    LastWrite Time Fri Mar 25 11:15:50 2016 (UTC)


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
 LastWrite Time Fri Mar 25 10:52:04 2016 (UTC)

 Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History
 LastWrite Time Fri Mar 25 10:52:04 2016 (UTC)
 ANALYST NOTE:
    No per-domain cookie decisions subkeys are present


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
 LastWrite Time Fri Mar 25 10:52:39 2016 (UTC)


*Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 LastWrite Time Fri Mar 25 10:54:20 2016 (UTC)
    (default)                       =
    AutoDetect                      = 0
    IntranetName                    = 1
    ProxyBypass                     = 1
    UNCAsIntranet                   = 1
    -- 'ZoneMap' subkeys -- not parsed:
      Domains                     Fri Mar 25 10:52:40 2016 UTC
      ProtocolDefaults            Fri Mar 25 10:52:40 2016 UTC
      Ranges                      Fri Mar 25 10:52:40 2016 UTC

Subkeys not parsed in 'Software\Microsoft\Windows\CurrentVersion\Internet Settings'

    Cache                 ---   Fri Mar 25 10:52:04 2016 UTC
    Connections           ---   Fri Mar 25 11:26:56 2016 UTC
    Http Filters          ---   Fri Mar 25 10:52:04 2016 UTC
    Lockdown_Zones        ---   Fri Mar 25 10:52:40 2016 UTC
    Passport              ---   Fri Mar 25 10:52:39 2016 UTC
    Zones                 ---   Fri Mar 25 10:52:40 2016 UTC
-----------------------------------------
javafx v.20110322
(NTUSER.DAT) Gets contents of user's JavaFX key

Software\JavaSoft\Java Update\Policy\JavaFX not found.
-----------------------------------------
listsoft v.20080324
(NTUSER.DAT) Lists contents of user's Software key

listsoft v.20080324
List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

Fri Mar 25 11:21:21 2016Z        ForceInterfaceCOM
Fri Mar 25 11:21:16 2016Z        Microsoft
Fri Mar 25 11:21:12 2016Z        Privax
Fri Mar 25 11:16:29 2016Z        RegisteredApplications
```
                                Page 8

```
                                Admin2 OUTPUT.txt
Fri Mar 25 11:15:51 2016Z       Yahoo
Fri Mar 25 11:03:16 2016Z       JavaSoft
Fri Mar 25 11:00:15 2016Z       Mozilla
Fri Mar 25 10:59:35 2016Z       Host App Service
Fri Mar 25 10:58:19 2016Z       OEM
Fri Mar 25 10:58:05 2016Z       Brother
Fri Mar 25 10:57:56 2016Z       Realtek
Fri Mar 25 10:56:31 2016Z       McAfee
Fri Mar 25 10:52:39 2016Z       AppDataLow
Fri Mar 25 10:52:22 2016Z       Wow6432Node
Fri Mar 25 10:52:13 2016Z       Intel
Fri Mar 25 10:52:06 2016Z       DashlaneUpgrade
Fri Mar 25 10:52:05 2016Z       Policies
Fri Mar 25 10:52:04 2016Z       Mine
-----------------------------------------
liveContactsGUID v.20110221
(NTUSER.DAT) Gets user Windows Live Messenger GUIDs

Software\Microsoft\Windows Live Contacts\Database not found.
-----------------------------------------
load v.20100811
(NTUSER.DAT) Gets load and run values from user hive

load
Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Mar 25 10:52:16 2016 (UTC)

load value not found.
run value not found.
-----------------------------------------
logonusername v.20080324
(NTUSER.DAT) Get user's Logon User Name value

Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Fri Mar 25 11:16:39 2016 (UTC)]
-----------------------------------------
mmc v.20080324
(NTUSER.DAT) Get contents of user's MMC\Recent File List key

Software\Microsoft\Microsoft Management Console\Recent File List not found.
-----------------------------------------
mndmru v.20080324
(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.
-----------------------------------------
mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Fri Mar 25 11:11:13 2016 (UTC)

Remote Drives:

Volumes:
Fri Mar 25 11:11:13 2016 (UTC)
  {1e043e47-febf-4b10-983a-321680f40f77}

Drives:
Fri Mar 25 10:52:20 2016 (UTC) - CPC
```

Page 9

Admin2 OUTPUT.txt
Unique MAC Addresses:
32:16:80:F4:0F:77

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices
entries that begin with "\??\Volume".
------------------------------------
mpmru v.20080324
(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.
------------------------------------
mspaper v.20080324
(NTUSER.DAT) Gets images listed in user's MSPaper key

SOFTWARE\Microsoft\MSPaper* not found.
------------------------------------
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
------------------------------------
nero v.20100218
(NTUSER.DAT) Gets contents of Ahead\Nero Recent File List subkeys

Software\Ahead not found.
------------------------------------
netassist v.20110427
(NTUSER.DAT) Check for Firefox Extensions.

Software\Mozilla\Firefox\Extensions not found.
Software\Microsoft\Windows\CurrentVersion\Uninstall\NetAssistant not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0 not found.
Software\Microsoft\Installer\Products\D4676621F4CF7AF46BB388D4351B86F0\SourceList
not found.

------------------------------------
odysseus v.20110202
(NTUSER.DAT) Extract registry keys for Odysseus by bindshell.net.

Software\bindshell.net\Odysseus not found.

------------------------------------
officedocs v.20080324
(NTUSER.DAT) Gets contents of user's Office doc MRU keys

officedocs v.20080324
MSOffice version not found.
------------------------------------
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version not found.
------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

MSOffice version not found.
------------------------------------
OSVersion
Software\Microsoft
LastWrite Time Fri Mar 25 11:21:16 2016 (UTC)
Page 10

Admin2 OUTPUT.txt

OSVersion value not found.
-------------------------------------------
outlook v.20100218
(NTUSER.DAT) Gets user's Outlook settings

Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
not found.
-------------------------------------------
policies_u v.20091021
(NTUSER.DAT) Get values from the user's Policies key


System\EnableProfileQuota value not found.
-------------------------------------------
printermru v.20091125
(NTUSER.DAT) Gets user's Printer Wizard MRU listing

Printers\Settings\Wizard\ConnectMRU not found.
-------------------------------------------
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Fri Mar 25 10:52:16 2016

   Microsoft XPS Document Writer (winspool,Ne00:,15,45)
   Microsoft Print to PDF (winspool,Ne01:,15,45)
   Foxit PhantomPDF Printer (winspool,Ne02:,15,45)
   Fax (winspool,Ne03:,15,45)
   Brother PC-FAX v.3.1 (winspool,Ne04:,15,45)
   Brother MFC-9340CDW USB (winspool,Ne05:,15,45)

Default Printer (via CurrentVersion\Windows): Brother PC-FAX v.3.1,winspool,Ne04:
-------------------------------------------
privoxy v.20110204
(NTUSER.DAT) Extracts the install path for Privoxy.

Software\Privoxy not found.

-------------------------------------------
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Fri Mar 25 10:55:06 2016 (UTC)
   CertificateRevocation          1
   DisableCachingOfSSLPages       0
   EnableNegotiate                1
   IE5_UA_Backup_Flag             5.0
   MigrateProxy                   1
   PrivacyAdvanced                1
   ProxyEnable                    0
   SecureProtocols                2688
   User Agent                     Mozilla/4.0 (compatible; MSIE 8.0; Win32)
   WarnonZoneCrossing             0
   ZonesSecurityUpgrade           1662196350
-------------------------------------------
publishingwizard v.20110202
(NTUSER.DAT) Extract AddNetPlace\LocationMRU for Microsoft Publishing Wizard

Software\Microsoft\Windows\CurrentVersion\Explorer\PublishingWizard\AddNetworkPlace\
Page 11

Admin2 OUTPUT.txt
AddNetPlace\LocationMRU not found.

------------------------------------
putty v.20110204
(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.

------------------------------------
rdphint v.20090715
(NTUSER) Gets hosts logged onto via RDP and the Domain\Username

Software\Microsoft\Terminal Server Client\Servers not found.
------------------------------------
realplayer6 v.20080324
(NTUSER.DAT) Gets user's RealPlayer v6 MostRecentClips(Default) values

Software\RealNetworks\RealPlayer\6.0\Preferences not found.
------------------------------------
realvnc v.20091125
(NTUSER.DAT) Gets user's RealVNC MRU listing

Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEX order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Fri Mar 25 10:55:21 2016 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs has no subkeys.
------------------------------------
rootkit_revealer v.20110204
(NTUSER.DAT) Extracts the EULA value for Sysinternals Rootkit Revealer.

Software\Sysinternals\RootkitRevealer not found.

------------------------------------
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Fri Mar 25 11:11:09 2016 (UTC)
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU has no values.
------------------------------------
Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
------------------------------------
shellfolders v.20090115
(NTUSER.DAT) Retrieve user Shell Folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
LastWrite Time Fri Mar 25 10:52:48 2016 (UTC)
!Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath
function instead
AppData              C:\Users\Mallik\AppData\Roaming
Local AppData        C:\Users\Mallik\AppData\Local
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Libraries
My Video             C:\Users\Mallik\Videos
                            Page 12

```
                                  Admin2 OUTPUT.txt
My Pictures            C:\Users\Mallik\Pictures
Desktop               C:\Users\Mallik\Desktop
History               C:\Users\Mallik\AppData\Local\Microsoft\Windows\History
NetHood               C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Network
Shortcuts
{56784854-C6CB-462B-8169-88E350ACB882} C:\Users\Mallik\Contacts
{00BCFC5A-ED94-4E48-96A1-3F6217F21990}
C:\Users\Mallik\AppData\Local\Microsoft\Windows\RoamingTiles
Cookies               C:\Users\Mallik\AppData\Local\Microsoft\Windows\INetCookies
Favorites             C:\Users\Mallik\Favorites
SendTo                C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu            C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Start Menu
My Music              C:\Users\Mallik\Music
Programs              C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs
Recent                C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Recent
CD Burning            C:\Users\Mallik\AppData\Local\Microsoft\Windows\Burn\Burn
PrintHood             C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Printer
Shortcuts
{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\Mallik\Searches
{374DE290-123F-4565-9164-39C4925E467B} C:\Users\Mallik\Downloads
{A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\Mallik\AppData\LocalLow
Startup               C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Administrative Tools C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
Personal              C:\Users\Mallik\Documents
{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\Mallik\Links
Cache                 C:\Users\Mallik\AppData\Local\Microsoft\Windows\INetCache
Templates             C:\Users\Mallik\AppData\Roaming\Microsoft\Windows\Templates
{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\Mallik\Saved Games
Fonts                 C:\Windows\Fonts


----------------------------------------
Software\Skype not found.
----------------------------------------
snapshot_viewer v.20110210
(NTUSER.DAT) Extracts Recent File List for Microsoft Snapshot Viewer.

Software\Microsoft\Snapshot Viewer\Recent File List not found.


----------------------------------------
ssh_host_keys v.20120809
(NTUSER.DAT) Extracts Putty/WinSCP SSH Host Keys

"Software\SimonTatham\Putty\SshHostKeys" does not exist

"Software\Martin Prikryl\WinSCP 2\SshHostKeys" does not exist
----------------------------------------
startmenuinternetapps_cu v.20101219
(NTUSER.DAT) Start Menu Internet Applications info current user

Software\Clients not found. Check the same path in HKLM
----------------------------------------
startpage v.20100330
(NTUSER.DAT) Gets contents of user's StartPage key

Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage
LastWrite Time Fri Mar 25 10:54:48 2016 (UTC)

StartMenu_Start_Time    = Fri Mar 25 10:52:19 2016 Z
----------------------------------------
streammru v.20090205
```

Page 13

Admin2 OUTPUT.txt

(NTUSER.DAT) streammru

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
----------------------------------------
streams v.20081124
(NTUSER.DAT) Parse Streams and StreamsMRU entries

Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU not found.
----------------------------------------
Software\SysInternals not found.
----------------------------------------
trustrecords v.20120716
Word

PowerPoint

Excel

Access

----------------------------------------
Launching tsclient v.20120827
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
----------------------------------------
typedpaths v.20100330
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths not found.
----------------------------------------
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Fri Mar 25 10:52:40 2016 (UTC)
  url1 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
----------------------------------------
typedurlstime v.20120613
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

Software\Microsoft\Internet Explorer\TypedURLsTime not found.
----------------------------------------
unreadmail v.20100218
(NTUSER.DAT) Gets contents of Unreadmail key

Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
----------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Fri Mar 25 11:01:40 2016 (UTC)
  OneDrive: "C:\Users\Mallik\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
/background
  Host App Service: "%LOCALAPPDATA%\Host App
Service\Engine\HostAppServiceUpdater.exe" /LOGON

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Page 14

Admin2 OUTPUT.txt
Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not
found.


Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Mar 25 10:52:16 2016 (UTC)
Run value not found.
run value not found.
load value not found.
------------------------------------
user_win v.20080415
(NTUSER.DAT)   --

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Mar 25 10:52:16 2016 (UTC)

------------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Mar 25 10:53:06 2016 (UTC)

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Fri Mar 25 11:23:33 2016 Z
  E7CF176E110C211B (33)
Fri Mar 25 11:21:03 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\HMA! Pro VPN\bin\HMA! Pro VPN.exe (1)
Fri Mar 25 11:15:27 2016 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Yahoo!\Messenger\YahooMessenger.exe (1)
Fri Mar 25 10:58:47 2016 Z
  Malwarebytes.ToastNotification (1)
Fri Mar 25 10:53:02 2016 Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.SkypeApp_kzf8qxf38zg5c!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (10)
  Microsoft.WindowsAlarms_8wekyb3d8bbwe!App (9)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)
Page 15

Admin2 OUTPUT.txt
   {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (6)
   Microsoft.Windows.StickyNotes (5)

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Fri Mar 25 11:23:33 2016 Z
   {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Mozilla Firefox.lnk (7)
Fri Mar 25 11:21:03 2016 Z
   C:\Users\Public\Desktop\HMA! Pro VPN.lnk (1)
Fri Mar 25 11:15:27 2016 Z
   C:\Users\Public\Desktop\Yahoo! Messenger.lnk (1)
Fri Mar 25 10:58:47 2016 Z
   C:\Users\Public\Desktop\Malwarebytes Anti-Malware.lnk (1)
Fri Mar 25 10:53:02 2016 Z
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (8)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (7)
   {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk (6)
   {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (5)

{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}

-------------------------------------------
userinfo v.20130513
(NTUSER.DAT) Gets contents of MS Office UserInfo values

Software\Microsoft\Office\Common not found.

Software\Microsoft\Office\Common\UserInfo not found.

Software\Microsoft\Office\11\.0\Common\UserInfo not found.

-------------------------------------------
userlocsvc v.20090411
(NTUSER.DAT) Displays contents of User Location Service\Client key

Software\Microsoft\User Location Service\Client not found.
-------------------------------------------
vista_bitbucket v.20080420
(NTUSER.DAT) Get BitBucket settings from Vista via NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
LastWrite Time Fri Mar 25 10:57:43 2016 (UTC)

LastEnum : 0,{1e043e47-febf-4b10-983a-321680f40f77}

{1e043e47-febf-4b10-983a-321680f40f77} [Fri Mar 25 10:58:16 2016] (UTC)
   NukeOnDelete     0
-------------------------------------------
vmplayer v.20110204
(NTUSER.DAT) Extracts full filepath for recent VMware Player VM images.

Software\VMware, Inc.\VMware Player\VMplayer\Window position not found.

-------------------------------------------
vmware_vsphere_client v.20110204
(NTUSER.DAT) Extract recent connections list for VMware vSphere Client.

Software\VMware\Virtual Infrastructure Client\Preferences\UI\ClientsXml not found.
Software\VMware\VMware Infrastructure Client\Preferences not found.

-------------------------------------------
vnchookapplicationprefs v.20110208

Page 16

Admin2 OUTPUT.txt
(NTUSER.DAT) Get VNCHooks Application Prefs list

Software\ORL\VNCHooks\Application_Prefs not found.
------------------------------------
vncviewer v.20121231
(NTUSER.DAT) Get VNCViewer system list

Software\ORL\VNCviewer\MRU not found.
Software\RealVNC\VNCViewer4\MRU not found.
------------------------------------
wallpaper v.200800810
(NTUSER.DAT) Parses Wallpaper MRU Entries

Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper\MRU not found.
------------------------------------
warcraft3 v.20110202
(NTUSER.DAT) Extract usernames for Warcraft 3.

Software\Blizzard Entertainment\Warcraft III\String not found.


------------------------------------
winlivemail v.20111118
(NTUSER.DAT) Get & display the contents of the Windows Live Mail key

Software\Microsoft\Windows Live Mail not found.
------------------------------------
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Fri Mar 25 11:27:02 2016 (UTC)
    FirstLogon = 0
    BuildNumber = 10240
    ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin;OneDrive;Work
Folders
    PUUActive = b5 a7 bd 5a 01 00 00 00 01 00 01 00 a8 07 00 00 a1 08 00 00 0c 33 00
00 d0 00 00 00 18 00 18 00 e3 97 52 5d 5d 33 00 00 6a 08 00 00 09 04 00 00 f9 02 00
00 63 00 00 00 af 03 00 00 55 08 00 00 62 00 00 00 04 00 00 00 0a aa dc 40 89 86 d1
01

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
    system had been infected with Bredolab (Symantec).  Also, check the
    contents of a "shell" value - should only include Explorer.exe, if
    it exists.
------------------------------------
winrar v.20080819
(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.
------------------------------------
winscp_sessions v.20120809
(NTUSER.DAT) Extracts WinSCP stored session data

"Software\Martin Prikryl\WinSCP 2\Sessions" does not exist
------------------------------------
winvnc v.20110202
(NTUSER.DAT) Extracts the encrypted password for WinVNC.

Software\ORL\WinVNC3 not found.
Software\ORL\WinVNC3\Default not found.
Software\ORL\WinVNC\Default not found.
Software\RealVNC\WinVNC4 not found.
Page 17

Admin2 OUTPUT.txt
Software\RealVNC\Default not found.

------------------------------------
winzip v.20140730
(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.
------------------------------------
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery not found.
------------------------------------
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

LastWrite Time Tue Apr 12 20:53:29 2016 (UTC) Pager
  Version            = 11.5.0.228
  Launch on Startup  = 1
  Connection Server  =
  Last Login UserName =
  Last Local IP      =
  AutoLogin          = 0
  Save Password      = 0
  Encrypted Password =
  Yahoo Token        =
  NOTE: you should not be able to obtain the password.

  LastWrite Time Tue Apr 12 20:53:29 2016 (UTC) profiles
  Found 1 users.
  Found 0 bad users logins.

  USER: callme_tim
  LastWrite Time Tue Apr 12 20:53:29 2016 (UTC) callme_tim
    LastWrite Time Fri Mar 25 11:15:54 2016 (UTC) Alerts
    Missing expected value 'Total Login Tries'
    Missing expected value 'Total Disconnects'
    LastWrite Time Tue Apr 12 20:53:29 2016 (UTC) Archive
    Missing expected value 'Enabled'
    Missing expected value 'Autodelete'
    NOTE: cannot determine archived messages policy due to missing values.
    Missing expected value 'CallHistoryEnabled'
    Missing expected value 'CallHistoryAutodelete'
    NOTE: cannot determine call history policy due to missing values.
    Missing expected 'FriendIcons' subkey.
    Missing expected 'FT' subkey.

------------------------------------
ALERT: user_run: Odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup

Page 18

SAM OUTPUT.txt

samparse v.20120722
(SAM) Parse SAM file for user & group mbrshp info


User Information
-----------------------
Username           : Administrator [500]
Full Name          :
User Comment       : Built-in account for administering the computer/domain
Account Type       :
Account Created    : Tue Mar 22 12:48:37 2016 Z
Last Login Date    : Thu Aug 13 22:56:42 2015 Z
Pwd Reset Date     : Fri Jul 10 12:22:01 2015 Z
Pwd Fail Date      : Never
Login Count        : 11
   --> Password does not expire
   --> Account Disabled
   --> Normal user account


Username           : Guest [501]
Full Name          :
User Comment       : Built-in account for guest access to the computer/domain
Account Type       :
Account Created    : Tue Mar 22 12:48:37 2016 Z
Last Login Date    : Never
Pwd Reset Date     : Never
Pwd Fail Date      : Never
Login Count        : 0
   --> Password does not expire
   --> Account Disabled
   --> Password not required
   --> Normal user account

Username           : DefaultAccount [503]
Full Name          :
User Comment       : A user account managed by the system.
Account Type       :
Account Created    : Tue Mar 22 12:48:37 2016 Z
Last Login Date    : Never
Pwd Reset Date     : Never
Pwd Fail Date      : Never
Login Count        : 0
   --> Password does not expire
   --> Account Disabled
   --> Password not required
   --> Normal user account

Username           : DeputyGod [1001]
Full Name          :
User Comment       :
Account Type       :
Account Created    : Tue Mar 22 13:12:30 2016 Z
Password Hint      : sara#
Last Login Date    : Thu Apr 21 03:19:31 2016 Z
Pwd Reset Date     : Tue Mar 22 13:12:30 2016 Z
Pwd Fail Date      : Tue Apr 19 00:27:33 2016 Z
Login Count        : 110
   --> Password does not expire
   --> Password not required
   --> Normal user account

Username           : Mallik [1002]
Full Name          :

Page 1

SAM OUTPUT.txt

```
User Comment      :
Account Type      :
Account Created   : Tue Mar 22 13:14:21 2016 Z
Password Hint     : #992
Last Login Date   : Fri Mar 25 10:51:56 2016 Z
Pwd Reset Date    : Tue Mar 22 13:14:21 2016 Z
Pwd Fail Date     : Never
Login Count       : 1
   --> Password does not expire
   --> Password not required
   --> Normal user account


--------------------------
Group Membership Information
--------------------------
Group Name      : Users [3]
LastWrite       : Tue Mar 22 13:14:21 2016 Z
Group Comment : Users are prevented from making accidental or intentional
system-wide changes and can run most applications
Users :
   S-1-5-21-670634337-3447264720-4152838973-1002
   S-1-5-4
   S-1-5-11

Group Name      : Event Log Readers [0]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Members of this group can read event logs from local machine
Users           : None

Group Name      : Guests [1]
LastWrite       : Thu Aug 13 21:54:47 2015 Z
Group Comment : Guests have the same access as members of the Users group by
default, except for the Guest account which is further restricted
Users :
   S-1-5-21-670634337-3447264720-4152838973-501

Group Name      : System Managed Accounts Group [1]
LastWrite       : Thu Aug 13 21:54:47 2015 Z
Group Comment : Members of this group are managed by the system.
Users :
   S-1-5-21-670634337-3447264720-4152838973-503

Group Name      : Distributed COM Users [0]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Members are allowed to launch, activate and use Distributed COM
objects on this machine.
Users           : None

Group Name      : Administrators [3]
LastWrite       : Tue Mar 22 13:14:40 2016 Z
Group Comment : Administrators have complete and unrestricted access to the
computer/domain
Users :
   S-1-5-21-670634337-3447264720-4152838973-1002
   S-1-5-21-670634337-3447264720-4152838973-1001
   S-1-5-21-670634337-3447264720-4152838973-500

Group Name      : Remote Management Users [0]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Members of this group can access WMI resources over management
protocols (such as WS-Management via the Windows Remote Management service). This
applies only to WMI namespaces that grant access to the user.
Users           : None
```

Page 2

SAM OUTPUT.txt

```
Group Name      : Performance Log Users [0]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Members of this group may schedule logging of performance counters,
enable trace providers, and collect event traces both locally and via remote access
to this computer
Users           : None

Group Name      : Performance Monitor Users [0]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Members of this group can access performance counter data locally
and remotely
Users           : None

Group Name      : IIS_IUSRS [1]
LastWrite       : Fri Jul 10 12:20:38 2015 Z
Group Comment : Built-in group used by Internet Information Services.
Users :
  S-1-5-17

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
     - S-1-5-4  = Interactive
     - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin

---------------------------------------
ALERT: user_run: Odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup
```

Page 3

SECURITY OUTPUT.txt

auditpol v.20121128
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time Fri Jul 10 12:20:37 2015 (UTC)

Length of data: 148 bytes.
```
0x00000000: 00 01 00 00 09 00 00 00 82 00 00 00 01 00 00 00   ................
0x00000010: 03 00 00 00 03 00 01 00 01 00 01 00 00 00 01 00   ................
0x00000020: 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00   ................
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000050: 00 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00   ................
0x00000060: 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00   ................
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000080: 01 90 05 00 0b 00 0e 00 03 00 05 00 06 00 06 00   ................
0x00000090: 04 00 04 00                                       ....
```
**Auditing is NOT enabled.
------------------------------------------
lsasecrets v.20140408
(Security) TEST - Get update times for LSA Secrets

Domain secret - $MACHINE.ACC
$MACHINE.ACC key not found
------------------------------------------
polacdms v.20100531
(Security) Get local machine SID from Security hive

PolAcDmS
Policy\PolAcDmS
LastWrite Time Thu Aug 13 21:54:47 2015 (UTC)

Machine SID: S-1-5-21-670634337-3447264720-4152838973

PolPrDmS
Policy\PolPrDmS
LastWrite Time Fri Jul 10 12:20:52 2015 (UTC)

Primary Domain SID: S-1-5-
------------------------------------------
ALERT: user_run: Odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup

Page 1

SOFTWARE OUTPUT.txt
Launching appinitdlls v.20130425
appinitdlls v.20130425
(Software) Gets contents of AppInit_DLLs value

AppInit_DLLs
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Jul 10 12:20:33 2015 (UTC)
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Jul 10 11:05:46 2015 (UTC)
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
-------------------------------------------
apppaths v.20120524
(Software) Gets content of App Paths subkeys

App Paths
Microsoft\Windows\CurrentVersion\App Paths

Thu Apr 21 03:28:00 2016 (UTC)
  javaws.exe - C:\Program Files (x86)\Java\jre1.8.0_91\bin\javaws.exe
Thu Mar 31 18:39:43 2016 (UTC)
  msoxmled.exe - C:\Program Files (x86)\Common Files\Microsoft
Shared\OFFICE12\MSOXMLED.EXE
Wed Mar 23 09:48:50 2016 (UTC)
  fsquirt.exe -
Tue Mar 22 11:54:21 2016 (UTC)
  mbam.exe - C:\Program Files (x86)\Malwarebytes Anti-Malware\mbam.exe
Tue Mar 22 11:02:38 2016 (UTC)
  PhotoshopElements.exe - C:\Program Files (x86)\Adobe\Photoshop Elements
2\PhotoshopElements.exe
Tue Mar 22 10:37:06 2016 (UTC)
  ois.exe - C:\PROGRA~2\MICROS~1\Office12\OIS.EXE
  winword.exe - C:\PROGRA~2\MICROS~1\Office12\WINWORD.EXE
Tue Mar 22 10:37:05 2016 (UTC)
  MsoHtmEd.exe -
  mspview.exe - C:\PROGRA~2\COMMON~1\MICROS~1\MODI\12.0\MSPVIEW.EXE
Tue Mar 22 10:37:04 2016 (UTC)
  excel.exe - C:\PROGRA~2\MICROS~1\Office12\EXCEL.EXE
  OneNote.exe - C:\PROGRA~2\MICROS~1\Office12\ONENOTE.EXE
  powerpnt.exe - C:\PROGRA~2\MICROS~1\Office12\POWERPNT.EXE
Thu Aug 13 22:39:52 2015 (UTC)
  foxitPhantom.exe - C:\Program Files (x86)\Foxit PhantomPDF\FoxitPhantomPDF.exe
Thu Aug 13 22:39:06 2015 (UTC)
  PowerDVD12 - C:\Program Files (x86)\CyberLink\PowerDVD12\PowerDVD12.exe
Thu Aug 13 21:54:53 2015 (UTC)
  firefox.exe - C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Fri Jul 10 13:19:49 2015 (UTC)
  cmmgr32.exe -
  IEDIAG.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
  IEDIAGCMD.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
  IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
  licensemanagershellext.exe - C:\Windows\System32\licensemanagershellext.exe
Fri Jul 10 13:14:46 2015 (UTC)

Page 1

SOFTWARE OUTPUT.txt
```
  Journal.exe - %ProgramFiles%\Windows Journal\Journal.exe
  mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe
  SnippingTool.exe - %SystemRoot%\system32\SnippingTool.exe
  TabTip.exe - %CommonProgramFiles%\microsoft shared\ink\TabTip.exe
Fri Jul 10 11:05:46 2015 (UTC)
  dfshim.dll -
  install.exe -
  mplayer2.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
  pbrush.exe - %SystemRoot%\System32\mspaint.exe
  PowerShell.exe - %SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe
  setup.exe -
  table30.exe -
  wab.exe - %ProgramFiles%\Windows Mail\wab.exe
  wabmig.exe - %ProgramFiles%\Windows Mail\wabmig.exe
  wmplayer.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
  WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
  WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths not found.
```
----------------------------------------
```
assoc v.20080815
(Software) Get list of file ext associations

assoc
Classes
```

----------------------------------------
```
banner v.20081119
(Software) Get HKLM\SOFTWARE.. Logon Banner Values

Logon Banner Information
Microsoft\Windows\CurrentVersion\policies\system
LastWrite Time Fri Jul 10 12:20:58 2015 (UTC)

Legalnoticecaption value =

Legalnoticetext value =

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Apr 21 04:41:14 2016 (UTC)

Legalnoticecaption value =

Legalnoticetext value =
```

----------------------------------------
```
bho v.20130408
(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
LastWrite Time Tue Mar 22 11:30:17 2016 (UTC)

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects has no subkeys.   No
BHOs installed.
Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
LastWrite Time Thu Apr 21 03:27:59 2016 (UTC)

Classes\CLSID\{02478D38-C3F9-4efb-9B51-7695ECA05670} not found.

Classes\CLSID\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43} not found.

Classes\CLSID\{DBC80044-A445-435b-BC74-9C25C1C588A9} not found.
```
----------------------------------------

Page 2

SOFTWARE OUTPUT.txt

bitbucket v.20080418
(Software) Get HKLM\..\BitBucket keys\values

Microsoft\Windows\CurrentVersion\Explorer\BitBucket *not found.*
-----------------------------------------
clsid v.20130603
(Software) Get list of CLSID/registered classes

Classes\CLSID

Thu Apr 21 03:19:25 2016 Z
    {54DD89C9-8CF5-41BC-BF34-F793A78B0331}   VulAdminAgent Class
    {5A973DFF-5D1E-4CCC-9072-2CDBDB5370A5}   ComMcVulAP Class
    {6B7015DC-CCB5-4133-8B9C-AF6721D6040F}   McVulProgressIcon Class
    {88FB3FDD-8644-4236-A8F7-F35BCFC627E2}   McVulAlert Class
    {B64EBEEB-A8B5-492F-B720-4E7E7005A717}   McVulDBUpdaterPlugin Class
    {FCFE95A1-AEB4-448E-8EA1-B711E21BE003}   VulUserAgent Class
Thu Apr 21 03:19:24 2016 Z
    {7DD30973-11DD-47B7-909A-69E5A36EC7C8}   McVulShim2 Class
    {B77D3416-5479-4AB7-96AC-5B8CB384E86B}   McVulVer Class
    {C38D6C58-29D0-4199-836B-2881AFD63C7E}   cWinUpdater Class
Thu Apr 21 03:17:30 2016 Z
    {9DC5AC69-B7D8-4DEB-A9EA-E8E2958BE7BD}   McVulController Class
Thu Apr 21 03:17:25 2016 Z
    {4C2F8A31-96A3-441F-9BE8-2A2E813F6FE5}   McVulODS Class
Thu Apr 21 03:15:49 2016 Z
    {0CB58125-ED4E-4125-B72E-BA3435AC4421}   PSFactoryBuffer
Thu Apr 21 03:15:48 2016 Z
    {5A90F5EE-16B8-4C2A-81B3-FD5329BA477C}   McAfee SACore Component
    {CD009C4C-EAAC-4A03-9C44-4342D4CFABA9}   McAfee Host SA Plugin
Thu Apr 21 03:15:47 2016 Z
    {0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064}   McAfee SiteAdvisor Toolbar
    {5513F07E-936B-4E52-9B00-067394E91CC5}   McAfee SACore Protocol Handler
    {B164E929-A1B6-4A06-B104-2CD0E90A88FF}   McAfee SiteAdvisor BHO
Thu Apr 21 03:15:46 2016 Z
    {0F5FA46A-D17B-4978-8A4C-65474C8DF59F}   SaSubMgr Class
    {21CBFEC0-E728-420C-B4A4-A58AD2089ABA}   McAfee SiteAdvisor saUpKeep
Thu Apr 21 03:15:28 2016 Z
    {C88F5D3A-EBE1-4513-AFC9-CE98CBD96A74}   ShredShlExt Class
    {EE480D09-9DD2-49A8-A3C3-B8B4B4F84F19}   PSFactoryBuffer
Thu Apr 21 03:15:27 2016 Z
    {31E65827-45A3-462A-A0CB-0B208F577152}   PSFactoryBuffer
    {674D81C2-E581-4235-B575-B6D22BB0B1B3}   McShredder Class
    {DA91E274-1702-419B-9871-EC6EFC62A355}   PSFactoryBuffer
    {F8855263-6377-4A95-8F34-40BFC158B038}   ShredderAPI Class
Thu Apr 21 03:15:26 2016 Z
    {629DEAAC-2F4F-4C37-95F0-16FC6EDD0C0E}   PSFactoryBuffer
    {861C8C71-ABFF-48A0-B8CE-A6E8B0CF53F0}   MQSProgressIcon Class
Thu Apr 21 03:15:25 2016 Z
    {2F4C0E0C-80AD-4105-9A0F-4BA90BB64296}   ApplicationInfo Class
    {32DE22BD-FA4F-42C4-AE35-A07A77F81098}   ThumbNailCallback3 Class
    {3E988004-1193-427E-8424-A2FB5BB29C87}   QuickClean Class
    {C2538E36-3135-49D9-B9D9-D5949FF1E949}   PSFactoryBuffer
    {C5FB18EF-94F5-43CA-ADCB-A9415F19207D}   McQuickclean Class
    {FA4E7235-687C-4D21-BC74-E10475FB9A8A}   QcAdmin Class
Thu Apr 21 03:15:17 2016 Z
    {AF6FB31C-95D0-4A0E-8AFE-099969D8B689}   McAfee Vaults
Thu Apr 21 03:15:12 2016 Z
    {9C156543-FD39-477E-96DB-A8B8F844D43C}   MATSysTrayPlugin Class
    {DCBAFCDA-3DC5-4D14-8E3F-8D1EC329F3E0}   PSFactoryBuffer
    {E57D5731-CD9F-4DC9-A122-60488A1EDD2E}   MATHelper Class
Thu Apr 21 03:15:11 2016 Z
    {71B7BFC6-B632-45B3-9D8B-9CBDA5B52E02}   PSFactoryBuffer
Page 3

SOFTWARE OUTPUT.txt
```
{D211A585-1DA6-42C2-86D2-082AC265776D}   MATProtectionShim Class
{F7520A2F-82E1-4DD5-A4BF-9D56BCF1D743}   MATApplicationInfo Class
Thu Apr 21 03:15:06 2016 Z
{B970338F-FDF9-45A2-B3F5-586C61BF5C1D}   McSvcSubsystem Class
Thu Apr 21 03:15:04 2016 Z
{19A34F98-20C0-4449-A3B4-29071BCEAD91}   MskOLAddIn Class
{C438913D-25B3-48cf-9310-9422CBCB19AB}   MskPlugin
Thu Apr 21 03:15:03 2016 Z
{E0EA5F46-A285-4ebd-9AA9-0CD334F5A9C5}   MSK OEMConfig
Thu Apr 21 03:14:58 2016 Z
{3087BEE5-7B7F-4C66-AB0B-5DCC65CD48A2}   CoMCAntispam Class
Thu Apr 21 03:14:57 2016 Z
{45559631-986C-4546-87E1-8AE1F9614296}   MSKSrgHelper Class
{516A0FE6-CA82-49F9-97EF-B5091F4B2E5A}   MskProtection Class
Thu Apr 21 03:14:43 2016 Z
{01BBDA6E-D5C6-47a0-AB4C-16E0FCA5009A}
{83748E14-8F60-4AB3-8A81-7CECBE2B1CBE}   MpsAppImpl Class
Thu Apr 21 03:14:42 2016 Z
{DE20B4BE-BD58-4304-BA1B-C9050CDF4B0C}   McParentalControls Class
Thu Apr 21 03:14:41 2016 Z
{08533142-6DAA-40C0-829F-098475E66646}   MpsPlugin Class
{12A5109E-F9A9-4A44-B849-2B6B245FC5EB}   MpsVersion Class
{B0F287F0-8024-4981-A6E9-A003641A61C3}   PSFactoryBuffer
{E9A45E1C-A219-416B-9E79-3C61B547209D}   mps
Thu Apr 21 03:14:39 2016 Z
{5AE43A84-811D-4aa7-96CC-41607ADE91EB}   Alert Class
Thu Apr 21 03:14:38 2016 Z
{09DBB645-8A30-4141-9ABE-826C1BBDFB10}   UserEvents Class
{14D12A5C-50FF-4fd3-9A4F-EF782812189F}   PSSignOutEventHandler Class
{229000A5-00F3-40b8-8984-F643C4C2952A}   PSKeywordBlockedEventHandler Class
{323826AD-B586-45b8-8E04-8736CBE1D670}   PSImageBlockedEventHandler Class
{49E62177-F1B8-4af7-AF05-1D8731E09A08}   SubscriptionEventHandler Class
{5C90092E-A90F-40F3-8155-49F087A3B752}   PSSignInEventHandler Class
{8C87D859-EFDC-40ae-9160-6918F459196C}   PSUrlVisitedEventHandler Class
{9395130C-49E0-462d-BC45-C1DBAC6B13A8}   PSAccessDeniedEventHandler Class
{9D3F632F-8427-4744-887B-6BD313EE61A6}   PSSignInRequiredEventHandler Class
Thu Apr 21 03:14:37 2016 Z
{7EB483B0-414C-4B45-A46C-CF4620531F8F}   McPrivacyServiceConfig Class
{94807D76-62F1-4C85-B794-D0B29E29DAAE}   MpsConfig Class
{99E69691-3266-4EA2-97FF-DFC40CF90DDC}   MpsLogger Class
{BD28FB5B-B2D0-4BA8-9755-618B29A95785}   UserHelper Class
Thu Apr 21 03:14:09 2016 Z
{447CAE10-7647-45f9-9AD8-68243ED5A2DA}   MpfpMCApplicationInfoProviderImpl Class
{820B1F90-F6DF-4f3a-9658-2A2E12F7B57C}   MpfpMCLogActionProviderImpl Class
{BD7EC3D0-8A8F-4ab8-9070-07997206D505}   MpfpMCRecentEventActionProviderImpl Class
Thu Apr 21 03:14:05 2016 Z
{5B2BB965-9043-498C-B60E-C0379DC0BBD4}   TrafficMonitor Class
{83EEF1DB-16A2-426F-843D-85A5348337C1}   MpfSvcImpl Class
{90DBDD22-4A4A-4b23-8BBC-969C9869E1D6}   MpfpAPIImpl Class
{C74C7A1D-476C-482A-B9D9-D76B50AFFFD4}   FirewallSettings Class
Thu Apr 21 03:14:04 2016 Z
{CF1B3E19-651E-4406-852B-9B7C4BABC82E}   PSFactoryBuffer
Thu Apr 21 03:14:03 2016 Z
{7585011C-0545-4F40-86B2-07639245F8ED}   MpfNdHelper Class
{C13F71BC-CC67-40A4-BEF2-1CBF44BD2A6D}   McAfee Personal Firewall MISP Alert
Thu Apr 21 03:14:02 2016 Z
{F8FDC79F-E062-48b0-946D-45DE13685593}   McAfee Personal Firewall OEM Configuration
Class
Thu Apr 21 03:14:01 2016 Z
{BA041363-3548-4CBA-BDB8-9338683BB8BC}   McAfee Personal Firewall Version Class
{F33B322A-8757-4E91-ACE3-28FE07AF968E}   PSFactoryBuffer
Thu Apr 21 03:14:00 2016 Z
{01A3B960-21A7-4231-909E-7597D17EF4A5}   McAfee Personal Firewall Application Class
```

SOFTWARE OUTPUT.txt
```
{60CCDA22-6301-439F-897B-08806DA744F2}  PSFactoryBuffer
{AAC05D4F-D3FC-4d85-B706-55ECE9CE6DCA}  McAfee Personal Firewall Configuration
Class
Thu Apr 21 03:13:56 2016 Z
{4E112792-FF8F-4f97-818B-2D7B9492F897}  MPFSubSystem Class
{DB4FBF4C-8F23-4FD5-97CB-84020AE74965}  McMPFSvc Class
Thu Apr 21 03:13:34 2016 Z
{76DEF3AC-2910-4234-9EE2-C81B2D45833A}  McAfee VirusScan Alerter
Thu Apr 21 03:13:33 2016 Z
{C98F04D7-CD30-4bb0-B7D7-8DD7448520F2}  McAfee MCODS
Thu Apr 21 03:13:30 2016 Z
{16453650-8364-4e9c-B891-1CF822B38F2E}  McAfee MCODS Shim
Thu Apr 21 03:13:29 2016 Z
{9d0f8731-12bb-42da-9a27-2f97b8c99998}  McAfee VirusScan Recent Events and Logs
Provider
Thu Apr 21 03:13:27 2016 Z
{0C146D72-9229-49D8-B2C9-D805EF5C69A9}  PSFactoryBuffer
{84D248DA-52CD-442c-B6AE-28F143DB1E33}  CoMcVSQuarantineAx Class
{89129896-0240-4245-A9F0-866E06263A0D}  McAfee McQuarantine Shim
{9EA1A0AD-B6AA-4f94-849C-02C8223CE619}  McAfee McRealtimeScan Shim
{A10DDD46-26AA-4b27-8FD1-D8A27A8AAF8C}  McAfee McTrustedItem Shim
{DE4F5EAE-49F5-BEED-DA6F-A387DE19EAF4}  McAfee RtsExclusions Shim
Thu Apr 21 03:13:26 2016 Z
{01576F39-90DE-4D6E-A068-5B20C22BAAEE}  CtxMenu Class
Thu Apr 21 03:13:25 2016 Z
{874f654b-c2a6-4f89-9195-6c6c3eeb779a}  McAfee VirusScan Application Information
Thu Apr 21 03:13:24 2016 Z
{33264B15-ECBD-4191-87A7-6B6422CB3A54}  PSFactoryBuffer
{44603E4D-56AE-4c42-ABE4-EC155FE8F1CD}  McAfee VirusMap Reporting
Thu Apr 21 03:13:23 2016 Z
{395633B1-EED9-4DFC-B67F-9788B51C9F06}  McAfee VirusScan Announcer Administrative
Class
{3EF62937-0A7B-4f6c-988D-994620390A80}  McAfee VirusScan Engine
{782C48A5-DD18-43E5-B32E-88E66CBB85D0}  McAfee VirusScan Announcer Alerter Class
{A737699F-3765-4B1D-ADAF-77424E23A9FA}  McAfee VirusScan Announcer Subsystem Class
{C90134D2-4AE9-407A-919A-4A2EF09C6C51}  MfeVsAnnServiceConfig Class
{DC7EF8E1-824F-4110-AB43-1604DA9B4F40}  McAfee VirusScan Announcer State Class
Thu Apr 21 03:13:22 2016 Z
{2813D8F5-E8CC-4102-B76A-472A0DF23E51}  McVSVer Class
{F80EAA49-6471-40B8-84F5-E1C1E4F5644A}  EscnPlug
Thu Apr 21 03:13:21 2016 Z
{94478404-6236-40C4-8850-DF09CE6D95BC}  PSFactoryBuffer
{D1646887-73BC-429E-A2D3-2299B684F91F}  McAfee VSO Setting Manger
Thu Apr 21 03:12:03 2016 Z
{1DD7B920-0AAE-457B-8A6B-077A92933F82}  McSvcSubsystem Class
Thu Apr 21 03:12:01 2016 Z
{89B3DCD8-9450-49DA-BFA4-7F9A6ED3B9A5}  PSFactoryBuffer
Thu Apr 21 03:11:45 2016 Z
{100A0E8F-D705-44AA-ABA7-842B96FA4ED9}  PEFSubDB Class
{6641D86E-79C2-42ED-9C08-BBDA2B780E1D}  PEFWebObjects Class
{B345DB9D-2FBE-4267-ADA2-5EFBFBF9C42F}  PCRegistry Class
{B97FDD09-7004-437E-9D5F-D336CB0F31A0}  CoUpdateMgrNotifyImpl Class
{E8C19781-29C1-4B08-9004-4F1BF947CCE9}  PCSystem Class
{ED71209D-F723-4ACB-BE33-1E5A79F9FEF3}  PCFile Class
Thu Apr 21 03:11:44 2016 Z
{DE4B86D4-00A1-463A-A26E-B7E555482952}  PefIntegration Class
Thu Apr 21 03:11:34 2016 Z
{62DD38CC-A2E4-43EA-92BA-5855CD2D60C1}  PSFactoryBuffer
Thu Apr 21 03:11:33 2016 Z
{255A5958-D283-4DD9-AA2E-8E33805CFC35}  McCSPClientAutomation Class
{58bf5ff7-38ff-46db-b7f3-dddee3f087cc}  McGenericCacheObject Class
{861CEB0E-B6F3-4DA8-A7E7-DBC43D335628}  PSFactoryBuffer
{8F2BC96B-68C5-40E8-9CE1-368E3ACAC09B}  McCSPClientShim Class
```
Page 5

```
                      SOFTWARE OUTPUT.txt
{A759F428-E51D-4CDF-8E4C-A52B7F9927D0}    McCDCObject Class
{B62A9F7D-4F97-4740-9EEE-3554F2AD2E4B}    McCSPClient Class
{E7BAC6B6-3FE3-4761-9471-F8F2C38C6C47}    McCDCObjectShim Class
{ecc2e0ca-e42a-4dcb-abe9-40a4e87d484a}    McGenericCacheShim Class
Thu Apr 21 03:11:27 2016 Z
{20966775-18A4-4299-B8E3-772C336B52A7}    McSurrogateHelper Class
{211EBA3A-EA5A-496b-A021-5C6BEB365E4C}    McAfee VirusScan ActiveShield
{3BAC5BDD-FCA1-4E2F-9062-6693E80016D8}    McPlatformServiceFramework Class
{4B3DBDAB-C46F-40D3-A415-3DB9585F4D00}    McUtilProvider Class
{85C12AD0-200B-48A0-9BEF-880ED5BE9D1D}    McPlatformService Class
{C307ED64-2933-4E7E-869B-7EFC8F6C7B18}    McAMTask Class
Thu Apr 21 03:11:26 2016 Z
{209500FC-6B45-4693-8871-6296C4843751}    ProtectionUIManager Class
Thu Apr 21 03:11:23 2016 Z
{F01E4065-20D6-4c86-9076-468AFB1B4156}    SessionMgr Class
Thu Apr 21 03:11:22 2016 Z
{6DFC2D17-579D-4c1c-93B7-B05B7DCCD766}    CoMcUpdateUI Class
{8F7EE58B-CEA5-4869-962F-AD58E4BD7465}    CoMcUpdateClientUI Class
{ADA518B9-B7A3-4C36-B4ED-49EB3FA189FC}    CoUpdateConnector Class
{E001E795-5A24-4E12-8B9C-6B80F190767D}    CoMcUpdateClient Class
Thu Apr 21 03:11:21 2016 Z
{E0EC0F2B-773D-4dd7-BE6C-7D85D6AA6269}    McAfee Agent
Thu Apr 21 03:11:19 2016 Z
{132DB361-34A1-43A3-9ECC-5BE245730365}    CoMcAlertMgr Class
{45F5697C-8C8C-4FDF-994E-C452372992E0}    CoAlertMgrAutomation Class
{4F8C7A2C-C891-400C-B4D7-A04D08CEF024}    PSFactoryBuffer
{E0827905-82D3-4566-ABA1-C67E4447F27E}    PSFactoryBuffer
Thu Apr 21 03:11:18 2016 Z
{A404171B-F5E6-40F5-8E35-90C616052B28}    PSFactoryBuffer
{abcdca3b-de6b-5a7c-b132-6d7cba63e5c5}    McIdleTaskAgent Class
{abceca3b-ea5a-496b-a021-5c6bab365e5c}    McAMTaskAgent Class
Thu Apr 21 03:11:16 2016 Z
{05C25B6F-5FC4-4E03-A330-F0F205FB2E9D}    CoMcTelemetryAPIShm Class
{26608B46-476A-4bf1-9CC6-AFEA28EBBC17}    McUserManager Class
{495DC25F-9EDE-47B4-968D-445A91B5C73E}    McSMProvider Class
{78A8678F-4F7E-4054-9B8C-B0E9136D6547}    Access to Analytics
{78EFC69B-FD0E-4F47-90D6-2FAD478C468D}    McDspRegistry Class
{8472B0B6-1510-4c08-B72F-1005782AF3D2}    McReportRecentEvent Class
{A8C5E344-038D-46D8-8B41-AED5C5BC9905}    McDspDatabaseMgr Class
{D38B2A0A-D751-4795-8CAC-DBCE8EF7D103}    PSFactoryBuffer
{D8736336-1BE6-4B07-82ED-76995CE281DE}    McDspFileSystem Class
{DDC6C82A-BCD6-480f-BAE7-9F406F687A53}    McReportLog Class
{DF659FF1-A244-4D36-9F84-75BB2D03EB2E}    McMscHelper Class
{E66D03F6-C1CF-4D8C-997C-FAE8763375F6}    ManageOem Class
{EEDAC291-85BC-488F-92DF-BA392D4AC6DE}    McDspSystemInfo Class
Thu Apr 21 03:11:15 2016 Z
{562E13B7-17D5-4393-A51E-BF1EFCB2AB13}    CoMcMLSMTKInfo Class
{678BABBE-FE1A-40A6-BB51-DFBF5F902E02}    CoMcReport Class
{80AD3138-435C-499B-A71F-7F129960E6F7}    PSFactoryBuffer
{9BB86057-19A1-49BB-A522-D4CE0AF55767}    CoMcIPTMgr Class
{A3D27DAD-37A4-496A-9553-2BD3E856899C}    CoMcMLSProv Class
{A557A096-4DA4-4E32-B863-BAFD39EEB367}    McPersonalization Class
Thu Apr 21 03:11:14 2016 Z
{2670E39B-AD89-451F-8220-DD8FC72E74D6}    McHistoryAndLogs Class
{3ED11E13-AB3A-49A1-B29E-B33853F6CB4A}    McUpdateSettings Class
{4FE2B7C8-AC9D-473C-A227-528F96CF0A88}    CoMcTOC Class
{F5DDF629-FAC9-4AA5-9BFF-EDA5FF8026AB}    CoMcTaskScheduler Class
Thu Apr 21 03:11:13 2016 Z
{071345B6-580F-47e5-A454-A76E9817CD8D}    CoMcAboutInfoCShim Class
{2C026D52-3200-44EF-A616-C6437A53AE45}    PSFactoryBuffer
{57249F09-6C95-43D5-977C-301EBAF7F3F5}    CoMcSecurityCenter Class
{5744BAD0-CB1D-43DB-90BD-1D2778CB0AD8}    CoMcMSCMiscellaneous Class
{72FA3944-C398-4300-BFAF-00F83A7F1B3E}    McMscHelper Class
```

Page 6

```
                           SOFTWARE OUTPUT.txt
     {7B3BE4B3-1ACA-40A1-B056-E01874B94975}   CoMcCategories Class
     {9BE580F3-3B6B-4101-923B-7D74D0D82B04}   CoMcProvHome Class
     {AD6E7ABF-E06F-4ff6-B734-D04F22DAE042}   CoMcMscCShim Class
     {B7D66A11-7233-4e29-A3B7-9D359344ED5B}·  CoMcInfoviz Class
     {BF1A6196-0201-41FF-9024-EBDCA65A2D85}   McGensettings Class
     {EC5F8EE1-A52B-4841-85C2-362990D50919}   CoMcCloudEventData Class
Thu Apr 21 03:11:12 2016 Z
     {4D13AE0B-CCCE-49AC-BB17-7BC48DDD7AA8}   PSFactoryBuffer
     {4D8E7AFE-514C-40eb-BBCB-ED0806F2E47E}   McEventDatabaseManager Class
     {5A40054F-2EBB-41bd-8A94-38C91AAFBC43}   McLogDatabaseManager Class
Thu Apr 21 03:11:11 2016 Z
     {524FFCA8-CE5C-4D65-A78F-716D1A403B1E}   CoMcServerContent Class
Thu Apr 21 03:11:10 2016 Z
     {95159ED8-48A3-4E84-9C75-550675F1F47F}   PSFactoryBuffer
     {CCA9EFD3-29ED-430A-BA6D-E6BBFF0A60C2}   McCtxFrmWrk Class
Thu Apr 21 03:11:09 2016 Z
     {3EF5086B-5478-4598-A054-786C45D75692}   McInternetProtocolRoot Class
     {6C92090B-807D-4473-8607-27A4449BFA74}   PSFactoryBuffer
Thu Apr 21 03:11:08 2016 Z
     {F6F390DB-9953-497B-B2F8-9F9B7C8A1B1C}   McUninstaller Class
Thu Apr 21 03:11:07 2016 Z
     {39BE9FE5-916F-4F01-86D8-46D1B843C8DD}   CCoMcApplicationInfo Class
Thu Apr 21 03:11:06 2016 Z
     {16D2A02D-7200-4AD7-97FA-BEEE9D3AF9FC}   PSFactoryBuffer
     {9BE8D7B2-329C-442A-A4AC-ABA9D7572602}   McSubMgr Class
Thu Apr 21 03:11:03 2016 Z
     {3C6B7AB4-14F6-49FA-93B2-536A7374C83A}   CUninstallCustomization Class
     {5C95C8F6-B4B4-47E7-9241-ECB5FA0A2C91}   PSFactoryBuffer
Thu Apr 21 03:11:02 2016 Z
     {61B085E5-356C-4fed-BEFF-AC6BE240B548}   CoMcApplicationRegistration Class
     {683C7EA1-3A4B-4764-A8E6-768C4F38BBA6}   PSFactoryBuffer
     {89CA5F54-B963-4092-873A-AFE498746367}   CoMcProviderRegistration Class
     {F2E467DC-4C6D-497c-A629-796B8CBF7275}   CoMCLogTemplateRegistration Class
Thu Apr 21 03:11:01 2016 Z
     {2CF7C0ED-0BC8-4CA5-AB2E-798E15D6EDDB}   IMcUIConfigMgr Class
     {5268CCA1-1270-4B04-B155-BD0753440278}   CompReg Class
     {9EFCE8D1-F3E0-460E-B301-0C08C95C1843}   PSFactoryBuffer
Thu Apr 21 03:11:00 2016 Z
     {11B6414A-7285-46BA-968E-1AD21C982109}   McAfee Event Registration
     {26016851-6AB3-449C-917F-198A8FB4FAE3}   McAfee Event Broker
     {DB112051-BFD7-4D32-AD3B-DF797F55A870}   McAfee Version
Thu Apr 21 03:09:42 2016 Z
     {9EBE7B1C-29B4-457A-A4FF-2883604805E0}   McAfee VSCore Version Class
Thu Apr 21 03:09:41 2016 Z
     {07AA2658-7A1A-47e5-B01A-701DC9EECD6F}   McHackerWatchFirewallSettings Class
     {0A9B27F1-F902-43a1-8663-BFF940E2F280}   RedirVer Class
     {0CE809D3-1D8B-4321-9F89-3F49CEA8B15C}   McHackerWatchServerQuery Class
     {0E3F1A07-DA76-4168-BA0F-4AFA3007CEFF}   EmProxyVer Class
     {231727DB-4A5A-4c85-B844-64E3A30BE7A3}   McHackerWatchAppDetails Class
     {36C29AB6-FF73-4f74-A2D1-C5C09B54E5C9}   McHackerWatch Class
     {6021CE48-B556-4f11-BC68-A647F056F8CC}   McHackerWatchVersion Class
     {858CCFAD-107A-4806-ACC4-68C84614EDDE}   McSvcSubsystem Class
     {85DADE1D-E53C-4E3A-8514-19FFB6B00423}   McHackerWatchAppEntry Class
     {A0EBB878-FDC0-4514-AEE9-F68E4337E7D2}   McHackerWatchSettings Class
     {D578D806-C260-4321-9AE0-3B181B39538C}   ProxyVer Class
     {FB49CFE3-C775-48f1-B0C6-BEBABF84EFF9}   McHackerWatchSharedPerms Class
Thu Apr 21 03:09:38 2016 Z
     {CEEEE239-EBC4-4780-A9EA-832D4634BCEC}   CoAlertLauncher Class
Thu Apr 21 03:09:37 2016 Z
     {090C890A-8E62-4324-954D-BCD2DFBE4E12}   Network Class
     {169C3F7A-F974-4B6B-BF09-DD7D08EAC3CE}   HomeNetVer Class
     {296CFB80-D8B3-44A4-B6B8-1931267F8F11}   ShimCallback Class
     {81375E2A-DBC6-4F93-A221-5DEE92D3A34C}   ShimList Class
```

Page 7

SOFTWARE OUTPUT.txt

```
{89105939-0E55-4F63-82F2-7EF170402AD1}   McAfee HomeNetwork Shim Component
{AF0CE3EB-8E31-4D61-98D4-A047F4826DE8}   ShimNetworkNode Class
{BBEDBE75-6E9C-40CB-8D3C-681E9F03807E}   McAfee HomeNetwork Service Module
{C28D8A9A-B234-4B23-8E31-1F4D1B9450CE}   ShimDynamicAttribute Class
{CBC58E3D-6DF2-4187-8188-CF9C261F1B89}   ShimProtectionProblem Class
Thu Apr 21 03:09:35 2016 Z
{A95B959F-64A9-43E4-A874-C8A77905854A}   CMcSvcHostVer Class
{C8C3A940-EE0E-4BFD-A151-E31A7F05F866}   PSFactoryBuffer
Thu Apr 21 03:09:07 2016 Z
{1091E03B-4449-452B-888F-3320936C3B30}   NotificationActivationCallback Class
Thu Apr 21 03:08:58 2016 Z
{AC29BAF7-7EFF-4A82-8B29-76B1A3E27A6D}   PSFactoryBuffer
{E782BE15-9936-4A7F-8DF9-9AB95D229DF1}   McClientAnalytics Class
Thu Apr 21 03:08:48 2016 Z
{15AF52F6-E83C-4228-95FE-4407687CEFBF}   CoMcUpdAgentUIHandler Class
{3C1CD4CD-9359-4A9D-A0FA-9E809E873CA6}   CoMcUpdateAgentCore Class
{590AB12E-F706-4BA8-9D08-A1EEC69A687D}   PSFactoryBuffer
{D905F5A4-15B0-4B47-99D8-CE0230557148}   CoUpdateMgrCore Class
{DA32C9C5-1147-402A-A127-E0E169E9E9B4}   CoMcUpdateAgent Class
Wed Mar 23 09:48:50 2016 Z
{0C39A5CF-1A7A-40C8-BA74-8900E6DF5FCD}
{2933BF90-7B36-11D2-B20E-00C04F983E60}   XML DOM Document
{3134ef9c-6b18-4996-ad04-ed5912e00eb5}
{3936E9E4-D92C-4EEE-A85A-BC16D5EA0819}   Frequent Places Folder
{5860E1C5-F95C-4a7a-8EC8-8AEF24F379A1}   CplPage Class
{59031a47-3f72-44a7-89c5-5595fe6b30ee}   UsersFiles
{62dc1a93-ae24-464c-a43e-452f824c4250}   WM LFX APO
{637c490d-eee3-4c0a-973f-371958802da2}   WM GFX APO
{C7386F3F-B5EB-4AF4-B261-5DCA3BEEF7B1}
Wed Mar 23 09:26:45 2016 Z
{80083BF3-B821-4cc2-AC62-81FAE8D3ADCE}   Brother Wia Scanner minidriver
Wed Mar 23 09:25:17 2016 Z
{9476E6F6-E582-40a4-BAF2-3D693AC88B6A}   Brother Wia Scanner minidriver
Tue Mar 22 13:31:12 2016 Z
{307523FA-DDC0-4068-983F-2A6B34627744}   ACloudToBeSynced Class
{5CCE71FA-9F61-4F24-9CD1-98D819B40D68}   ACloudSynced Class
{C1E1456F-C2D8-4C96-870D-35F1E13941EE}   ACloudSyncing Class
Tue Mar 22 13:15:31 2016 Z
{223A2D27-0448-4247-B4AC-DE846A23C71E}   DriverInterface Class
{81719F80-8503-4AA6-99F6-EDD8353B6CD4}   DPTopologyInt Class
{9B5F5829-A529-4B12-814A-E81BCB8D93FC}   TheDeskTopContextMenu Class
{A8CB24B9-7B0B-462F-A2B7-48746020A43D}   CUIString Class
{D5F5053A-9585-4D80-8F6F-7B6587CEFB93}   DataHandler Class
{FA507C3F-30C6-4DCA-9EE5-2656072EEC14}   TheAdvOSPropPage Class
Tue Mar 22 11:54:23 2016 Z
{57CE581A-0CB6-4266-9CA0-19364C90A0B3}   MBAMShlExt Class
Tue Mar 22 10:34:58 2016 Z
{1F2FD001-0148-474e-843E-D6D37A848D62}   Microsoft Office OneNote Windows Desktop
Search IFilter Base Class ID
{4887767F-7ADC-4983-B576-88FB643D6F79}   Office Open XML Format Excel Persistent
Handler
{4F46F75F-199F-4C63-8B7D-86D48FE7970C}   Office Open XML Format PowerPoint
Persistent Handler
{D3B41FA1-01E3-49AF-AA25-1D0D824275AE}   Office Open XML Format Word Persistent
Handler
{FB10BD80-A331-4e9e-9EB7-00279903AD99}   Office Outlook MSG Persistent Handler
Tue Mar 22 10:34:57 2016 Z
{4039B326-9F27-4B4A-B460-47A0C6A39D5C}   Office Outlook MSG IFilter
{42042206-2D85-11D3-8CFF-005004838597}
{506F4668-F13E-4AA1-BB04-B43203AB3CC0}   ImageExtractorShellExt Class
{5A98B233-3C59-4B31-944C-0E560D85E6C3}   Office Open XML Format Word Filter
{6D01EC38-83F9-45df-99F0-8A880993928D}   Microsoft Office OneNote Windows Desktop
Search IFilter
```

Page 8

SOFTWARE OUTPUT.txt
```
{72773E1A-B711-4d8d-81FA-B9A43B0650DD}    Microsoft Office OneNote Windows Desktop
Search IFilter Persistent handler
   {807563E5-5146-11D5-A672-00B0D022E945}    Microsoft Office InfoPath XML Mime Filter
   {88D969E5-F192-11D4-A65F-0040963251E5}    XML DOM Document 5.0
   {88D969E6-F192-11D4-A65F-0040963251E5}    Free Threaded XML DOM Document 5.0
   {88D969E7-F192-11D4-A65F-0040963251E5}    XML Schema Cache 5.0
   {88D969E8-F192-11D4-A65F-0040963251E5}    XSL Template 5.0
   {88D969E9-F192-11D4-A65F-0040963251E5}    XML Data Source Object 5.0
   {88D969EA-F192-11D4-A65F-0040963251E5}    XML HTTP 5.0
   {88D969EB-F192-11D4-A65F-0040963251E5}    Server XML HTTP 5.0
   {88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}    SAX XML Reader 5.0
   {88D969EE-F192-11D4-A65F-0040963251E5}    SAXAttributes 5.0
   {88D969EF-F192-11D4-A65F-0040963251E5}    MXXMLWriter 5.0
   {88D969F0-F192-11D4-A65F-0040963251E5}    MXHTMLWriter 5.0
   {88D969F1-F192-11D4-A65F-0040963251E5}    MXNamespaceManager 5.0
   {88D969F5-F192-11D4-A65F-0040963251E5}    MXDigitalSignature 5.0
   {8DE0A0A1-96D0-4B04-8EC6-2DBF9BD888DC}    QuickViewShellExt Class
   {993BE281-6695-4BA5-8A2A-7AACBFAAB69E}    Microsoft Office Metadata Handler
   {A394DCA9-3727-11D4-BD85-00C04F6B93A4}    CVisioFileFilter Class
   {AB968F1E-E20B-403A-9EB8-72EB0EB6797E}
   {B8D12492-CE0F-40AD-83EA-099A03D493F1}    Microsoft Office OneNote Filter
   {C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97}    Microsoft Office Thumbnail Handler
   {D66DC78C-4F61-447F-942B-3FB6980118CF}    CInfoTipShellExt Class
   {DDFE337F-4987-4EC8-BDE3-133FA63D5D85}    Office Open XML Format PowerPoint Filter
   {E772CEB3-E203-4828-ADF1-765713D981B8}    Microsoft Office OneNote Section
persistent handler
   {EDA26AA4-13EE-4304-8115-F7A5AE41D72F}    Microsoft Office OneNote Windows Desktop
Search Protocol Handler
   {F5BF6FE9-913F-4117-94C7-5040C7E3A6C1}    IconHandlerShellExt Class
   {F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}    Office Open XML Format Excel Filter
Thu Aug 13 22:52:19 2015 Z
   {645FF040-5081-101B-9F08-00AA002F954E}    Recycle Bin
   {679f85cb-0220-4080-b29b-5540cc05aab6}
   {a5a3563a-5755-4a6f-854e-afa3230b199f}    Library Folder
Thu Aug 13 22:51:29 2015 Z
   {1839FA17-C749-45B8-90FF-583264504803}    MccSPSettingsManager Class
   {2069B537-D856-4638-BC14-99745B90470C}    MccSPSettingsManagerShim Class
Thu Aug 13 22:39:52 2015 Z
   {21F5E992-636E-48DC-9C47-5B05DEF82372}    Foxit PDF Thumbnail Handler
   {3D50EEF1-10FF-44DE-B98E-A8C6E90CD26C}    OutlAddin Class
   {81D3C1A7-1155-41A3-9FD4-9D772CEFFFD5}    WordAddinPH Class
   {C350B0F1-6F74-410E-82E8-739CF4943B40}    PPTAddinPH Class
   {C5269811-4A29-4818-A4BB-111F9FC63A5F}    ConvertToPDF Class
   {E80C3EB2-92DF-4380-9BE7-0C6CC17A43D0}    ExcelAddinPH Class
Thu Aug 13 22:33:48 2015 Z
   {BD6ECB00-7C4A-4F97-B425-44117F2A7AAE}    The Amazon 1Button App for Internet
Explorer
   {E4ADC61E-D06A-4E0E-8582-78C809CC8450}    GadgetWindow Class
Thu Aug 13 22:33:03 2015 Z
   {148D5E31-0D7E-44EE-B5C2-291B822351EA}    TheGfxUILauncher Class
   {495BFA36-B75D-4565-8C75-3A583E8BF65D}    HotKey Class
Thu Aug 13 22:33:02 2015 Z
   {5DC5B31E-0C28-4679-B8D8-32CF2F9BACED}    PSFactoryBuffer
   {7160A13D-73DA-4CEA-95B9-37356478588A}    CUIExternal Class
   {F0BD5888-B756-4F3E-A4BA-8B7D9078C838}    TrayMenu Class
Thu Aug 13 22:30:56 2015 Z
   {1314AA9D-5AF7-4f1f-AD10-734156E1FF73}    DolbyDigitalLive Class (Analog)
   {1DCF439D-B5D6-436B-A9EB-6847EA9B9940}    DTSS2HeadphoneCoClass Class
   {3652DCDC-70DA-46FB-9B81-F0938731EE44}    DTSBoostCoClass Class
   {56E00778-C664-4bb5-AA2B-CA6F14840BB3}    EE GFX Analog Class
   {7F56EE63-86CA-4BD3-9C3B-85E84A6C0373}    DTSBassEnhancementCoClass Class
   {7FF7D60E-D129-4061-AEC9-D8477A4F9748}    SFSSAPOGFX Class
   {8C4BEBA7-72FE-4ed3-86CF-9760915AE13D}    Dolby SRC Class (Analog)
```
Page 9

SOFTWARE OUTPUT.txt

```
{91AA17F8-8A7E-4E11-8389-EAA92FC2A9C5}    DTSLimiterCoClass Class
{958342AF-451A-4443-9CFE-55679A2DD524}    PCEE4 ASL Analog COM Class
{A1B78981-4E84-4C0D-AE67-EF173688221C}    DTSVoiceClarityCoClass Class
{BC799B8B-08FC-4034-84BB-7B1B4EC32671}    DTSSymmetryCoClass Class
{BC8E3B67-3306-4eef-B230-6798E9A67F0B}    EE LFX Analog Mainstream Class
{BC95C973-E2C1-4df5-8878-6CCE0CB568FE}    DolbyPCEE4 Class (Analog)
{BE79D50C-73D1-4C1A-8A4B-79A5E000FA87}    DTSNeoPCCoClass Class
{C214B418-0813-46A7-9CB1-BE18206B7770}    DTSINPUTLFX Class
{C53E5AAF-5F6F-41c2-9F63-ADEBBC9B6B64}    EE P Analog Class
{C5BB45D1-B0C8-4907-AFDA-05A099F4CFDD}    DTSOUTPUTLFX Class
{C79BA6D1-F7B8-4b87-A405-ED9DE29A8B6D}    DTSGFX Class
{CBEB14A0-9B78-41BC-97D5-EA649DBB338D}    DTSS2SpeakerCoClass Class
{CDF59A71-0826-4812-B529-2E04D1497193}    DTSOUTPUTGFX Class
{CEDCD345-8C2C-4928-B8C9-AE867372A7CF}    DTSLFX Class
{D1219BD5-B542-4ab7-82CB-C89DDA9F3768}    DTSGFXNS Class
{E14FE766-9138-4e7f-99BE-7170114916A3}    KnowlesAPOGFX Class
{E14FE767-9138-4e7f-99BE-7170114916A3}    KnowlesAPOLFX Class
{F6F218EB-D925-43C7-BD4A-200ED278E81D}    DTSGainCompensatorCoClass Class
Thu Aug 13 22:30:55 2015 Z
{001348B9-D4F7-4008-A509-DFAE98D73CD0}    DolbyINV Class (Analog)
{00D816D5-A576-4884-8DBA-589D3FF1D371}    Dolby Digital Plus API COM Class
{04CB2171-695B-41CD-A3BE-5A3B92254A84}    YamahaAE
{08FD8A78-64B6-4692-96D2-1A363A7E3B9A}    EE P Analog Netbook Class
{0DC39FF3-7F96-405e-BC77-1323866D97CF}    DolbyDigitalLive Class (Analog)
{0E055C6A-5E79-431F-9BD3-F3D1DC78210D}    Dolby Digital Plus Class (Analog)
{11825B7C-5AA6-4E2F-A4BC-67659568E925}    SRSPremiumSound Class
{137A78D3-65B7-4e2f-851C-6EC4B633B436}    EE P Analog Premium Class
{147BF94E-33F9-4d26-BCF7-B0BD3AE09367}    AEAudioAPOLFX Class
{23A98C03-FA1E-4137-ADC7-9CFA50A833E4}    ICEsoundAPOMFX Class
{23FCAEEC-4AB9-4381-AAC5-CBF07F3DD1C4}    YamahaAE
{28636DCB-D4EC-49f2-AE04-F87F6AAA9825}    SFAPOLFX Class
{33330000-3657-4da7-96d6-9c0808ca95a6}    MaxxVoiceAPOPSS Class
{33330001-fcfc-4367-9e0e-5d4533ff7dcb}    MaxxVoiceAPO Dock Class
{33333337-c9bd-47cd-8a2d-de4341773869}    MaxxVoiceAPOLFX Class
{340DAC03-D632-449d-A211-4182115FA4D3}    DolbyProLogicIIx Class (Analog)
{351E24C9-25D8-4bcd-8E00-CA407967AA40}    AEAudioAPOGFX Class
{35D7A7FA-8AB2-401c-983E-919903F5D5AD}    EE P Analog Mainstream Class
{40BA376E-C60E-441B-BFCD-03F6DDB16552}    Dolby Digital Plus P Analog Class
{438993C7-7745-4137-99D3-C1E9402AE4F7}    Dolby Digital Plus Analog Mainstream Class
{44444400-3f0b-402a-af67-8244f1075962}    MaxxVoiceAPO A Class
{44444401-d66f-4826-824a-63974a0d27ad}    MaxxVoiceAPO B Class
{44444402-aed6-4172-9884-14e02f2a7d72}    MaxxVoiceAPO PSS Class
{44444403-c7e3-40c4-94eb-8d5f3fabb3e8}    MaxxVoiceAPO Dock A Class
{44444404-dbc0-4106-91ed-87aa08bf614e}    MaxxVoiceAPO Dock B Class
{5179399B-B5C4-4E79-8C02-D1D3E108EA8E}    SFAPOEFX Class
{5A6CE46A-0DE0-446d-8190-5EEF6A56E819}    SFAPOGFX Class
{5D062D6A-4D8D-405c-9D41-36517A79D799}    DolbyHeadphoneII Class (Analog)
{649B02ED-D042-44A5-A155-90276859DE78}    ICEsoundAPOEFX Class
{66660000-626b-4aea-b582-5895aeddf39f}    MaxxAudioAPO B Class
{66660001-81f3-42cd-9a32-5c72273431fe}    MaxxAudioAPO Dock A Class
{66660002-06d0-4b9d-a121-775aa4ac208f}    MaxxAudioAPO Dock B Class
{666666de-de1f-47e6-a4c4-dba360675157}    MaxxAudioAPO Class
{697A25AB-7233-4E22-A6AB-896387D1980F}    ABIT Class
{6C77EE15-11FE-4689-9814-C25DC3B9226E}    EE GFX Analog Mainstream Class
{77777700-a618-46a1-b783-f50fdba00e86}    MaxxAudioAPO Class
{77777701-ff66-4d7e-939c-3859cafbe669}    MaxxAudioAPO B Class
{77777702-4bd6-4e10-bf93-391d0413305f}    MaxxAudioAPO Dock A Class
{77777703-9a73-44bb-bfe9-db76354b330e}    MaxxAudioAPO Dock B Class
{8F3540DF-18B0-4943-B916-D4A79801587D}    SEAPOEFX Class
{9180EC39-FC40-4cee-9F0D-2398771A544E}    EE GFX Analog Premium Class
{A8004167-E235-4148-A4E5-7C3108100200}    CnxtDspGFX Class
{A9C2CEBF-36DC-40A3-92E6-ED59FDD9D20D}    SONY Class
{AA4CE0BA-E016-4FE4-B44C-3E4208100200}    CnxtDspLFX Class
```

Page 10

SOFTWARE OUTPUT.txt

```
{ABC87F6A-B935-4E6C-AED1-B9A443E3E47E}   EE LFX Analog Mainstream Class
{AF099A7C-45D2-4CE6-9327-EEAAB0395444}   RtkCfgApi Class
{bdf92412-5835-11e4-8ed6-0800200c9a66}   NAHIMICV2 LFX Class
{bdf92413-5835-11e4-8ed6-0800200c9a66}   NAHIMICV2 APO GFX Class
{C26AD82E-B1CB-4BDF-87E9-CACD7FD6C6FD}   SEAPOGFX Class
{C6606CA5-2108-4CAF-8E52-1953F2DBF716}   PropSet Class
{CC0CA09A-5B84-43F2-BE5C-9169C192565F}   RTLCSSAPI Class
{CF74FB2A-DBB2-4c8d-9C8E-0424AB05C810}   DolbyTDAS Class (Analog)
{D5FBCBC7-C56D-4FF0-9607-1B68B7EE02E2}   ICEsoundAPOGFX Class
{D6B23B09-BBB6-43a2-837F-BB2AA9237A30}   DolbyPCEE3UseCase Class (Analog)
{DF76A088-FD7D-4f4e-AAA1-626606B2419F}   EE LFX Analog Netbook Class
{E23C746E-3A9D-4040-8C85-6BBB044B73C7}   EE LFX Analog Premium Class
{E32A710E-8693-44e2-87FF-6B578E845C50}   DolbySRC Class (Analog)
{E9F1F599-7B14-4213-BF46-F992758CAB81}   RtlCP Class
{F55F3B53-36AD-4F8A-BF31-C5E776F7B00C}   TosSAEMAXAPO Class
{F71CA881-A2E0-43D1-9B8D-CEF14AA0D58D}   SEAPOLFX Class
Thu Aug 13 22:30:54 2015 Z
{0230C6C9-7038-4E8F-942D-D0316F813BAB}   TosSAEAPO Class
{048E5288-25FF-4552-BFE0-A9B7DE629CBA}   DsrApi Class
{073E187F-BB72-4d0f-8368-C6A20CD9EA50}   ForteProcModeApi Class
{07817D83-3E7B-4420-8541-2B37E76F6012}   MISSAPOLFX Class
{0bdc9ab6-78ed-11dc-8314-0800200c9a66}   SwapAPOGFX Class
{0D490185-0EF5-4E25-9994-EF95218A851C}   SRS_LFX_APO_Universal Class
{0E249A19-94DF-418A-9191-41D1FA0F3C2E}   RtkApoNotification Class
{0F40A6BB-F083-4B90-B69F-2993B14E2AD6}   SRSAPOConfigProperty Class
{10E241D3-EA1B-4edf-BFB5-61B7055C9DF0}   DtsApoBtPage Class
{11111155-852c-48b9-8d43-61e5455392d3}   MaxxSpeechAPOLFX Class
{130D6967-A060-4231-892A-933475EE2CB2}   SrsLaunchPage Class
{134DDB7A-41FC-40E6-8D6B-E284C51D160E}   DTS_MFX_APO Class
{19FF3488-2F16-409b-8FDA-B99181718FF6}   TADEFxRender Class
{1B917FE2-47D1-425D-A26E-AFCDBDA7A2E8}   DTS_SFX_APO Class
{1D1708DE-F500-4402-92ED-5CA693DABE72}   DLitePageHDMI Class
{1F76D7C4-58D0-43B8-BFD9-29EB23C71F4B}   SRS_HP360 Class
{22220001-5ee5-4a88-9c52-cc2989d6ac6d}   MaxxVoiceAPO Dock Class
{22222283-f501-4114-a51f-04b318d992e4}   MaxxVoiceAPOLFX Class
{22DF4E87-F39A-4cbd-988C-BF3F49CDA965}   MaxxAudioAPOLFX Class
{248F37DE-5F40-4dc6-9B51-3A14C1D71FD5}   DPCEE3RApi Class
{24A06156-8EC3-4d0b-85D1-41CB0831DA1C}   XearPage Class
{266ADF9D-0053-4228-B1DD-B09177D552C0}   Dolby Digital Plus Class (Analog)
{2896004F-3AAB-4A25-8C81-846E659BB1EE}   TosASFAPO Class
{2AB3AD17-438A-463F-99A7-3FD1DCF44BF5}   AnalysisData Class
{2C5F70F1-FAA2-4D71-918C-9174613909B6}   TepeqAPOGFX Class
{30543F69-1213-4284-9D0A-5CE5F71A82CD}   DhtApi Class
{30CB44E2-8BC1-44bd-A6DD-2E58E2365CC8}   DtsApoConnectPage Class
{31929B1C-6E3C-431c-A20D-2A2A8315344D}   RtkRecOptionsApi Class
{31A53A7B-E0D8-4f99-B950-F6C8F25E6731}   AdvEndpointPropPage Class
{3739576F-F27B-4857-9E3E-8BAAA2A030B9}   RtNuanceProc Class
{3833A070-8C55-4465-9B8F-BDBE0C6498B8}   RtkRec4StreamApi Class
{38361248-B055-4ea8-A373-940464FB318E}   SAApi Class
{39A8813E-9F8F-4735-BDFD-D067FFEE94E1}   SelHwEqPage Class
{3A2B839D-6060-4711-B3A8-35132A881E78}   DPCEE3Api Class
{3A40ED31-B1EB-4905-8A9A-7B65F78541BE}   RtkCapVoicePage Class
{3AD5DEB0-D8F8-424f-8391-8C7A257F6310}   SRSTruSurroundXTBlock Class
{3C8BA013-2AA8-4687-8913-4EA83E269AE8}   SRS_LFX_Capture_APO_Universal Class
{42D0571B-9239-4eee-B8A0-1C8B85608894}   DTSUP2Api Class
{42F7121A-9917-4927-9E44-C9B305B0EDBB}   RtkSRSPSApi Class
{43306DF8-E185-415d-BA78-D50E337921FA}   ForteRenderPage Class
{43B6893E-1071-432B-968E-DD683ADA6589}   AndreaPropPage Class
{44440000-c661-4f31-a1a4-94937c15c087}   MaxxAudioAPO B Class
{44444440-42ce-433f-9992-8eb7976b907b}   MaxxAudioAPO Class
{444D30F3-998E-41AE-A182-57B60AB9F783}   TosEAEAPO Class
{44EE5F71-5DD2-4434-B1AA-16B850F4BEC5}   SounzVoizApi Class
{45750165-6E3D-4413-AEE0-D486BC169E0B}   TAdeApi Class
```

Page 11

SOFTWARE OUTPUT.txt

```
{46D50ACF-34CA-4dfd-ACC8-481F6E686936}    Rtk3DHpPage Class
{498A0C2A-D4C5-4cbb-B62F-FB075A02F5A8}    MCEQApi Class
{4D7F2D1E-6D4E-4B4F-9F94-07035251339A}    SRSAPOConfigEnumerator Class
{54E2FC61-FA9E-4667-BC4B-005BD2EF3EA1}    Dolby Digital Plus API COM Class
{55550001-9c76-457f-b3d2-a1400b696958}    MaxxAudioAPO Dock A Class
{55550002-a639-4dc2-b816-21158f7cb9ed}    MaxxAudioAPO Dock B Class
{55550017-0c8d-4bac-baf2-24ac14b873e2}    MaxxAudioAPO B Class
{55555548-68cc-4cd7-b0b1-e5744039e781}    MaxxAudioAPO Class
{5680B311-447E-4fb6-B327-3C9B50A56FE3}    CEPage Class
{5B05A596-33CA-4D65-B6C8-42704CA9BE2A}    MaxxAudioApi Class
{5DE0635D-0C4A-4651-B00F-A1A87A2A5BBF}    DolbyPropPage Class
{5E2663C1-51B3-49B7-B081-70181C2AF816}    SRSTruSurroundXT Class
{5F4F9B2A-5992-4005-9714-021EBC439E9A}    DtsApoSyPage Class
{6201C0B0-A1DC-4AE2-9665-8DAB2E380073}    DolbyApi Class
{62AF1550-7402-42c2-8B94-9C644780F3AC}    SF3LinkPage Class
{63B28B9D-5064-496E-9729-8DF838C82656}    SRSAPOControlEnumerator Class
{6861CFDC-0461-49d5-A8DF-BE5ACD02692F}    RtkAdvPropPage Class
{68E6DF30-3484-489b-8120-3C4C0256A758}    RtkApoCommonApi Class
{6DECA3ED-3EEB-4ebd-8255-74686F53D707}    SoundAlivePage Class
{6FC60FF9-EDBB-47B5-9496-05D00561EF4B}    ExtDspPropPage Class
{70306ef0-7851-11dc-8314-0800200c9a66}    SwapAPOCAP Class
{71833FDE-B66B-44aa-8993-5512920C1B4F}    Knowles2Page Class
{727120C0-5689-4e6d-AFC0-E9762ABC32B8}    MaxxAudioPage Class
{72DA76A6-046C-4f1b-B7DD-4595A5ECF375}    DolbySPage Class
{735CBF5A-7149-4d58-B35C-AFE4862A2311}    DtsApoUpcPage Class
{7505CB57-3A77-46a4-8B04-75897B0AA643}    RtkOmniSoundApi Class
{7A84CB1C-5B82-4999-B028-D19EA3004D77}    RtkAM3DApi Class
{7B4BF64E-D05D-481D-97CC-C0829AC9280F}    DTS_EFX_APO Class
{7ECCA61E-6028-4afa-B03C-B68004412CAF}    RtkBassBackApi Class
{7F35C5D8-A7A7-4E6F-8ADB-E695EF0035E9}    APO3MainPropPage Class
{818BAAC5-A5A2-4A49-B9D4-C7274E946132}    SRSOperatingMode Class
{818D2D10-8A8C-4270-B044-AF1A5759D73C}    RtkRenderNsPage Class
{8338CED2-0837-11dc-8314-0800200c9a66}    SwapAPOGCAP Class
{853B15F2-A9DE-4592-9FA9-7A69F6AEA6A2}    DPCEE4Api Class
{8852ECE8-595D-427E-B5A0-F8D2E62FABBD}    SrsApoPropPage Class
{88A0B959-0AAC-486e-90EC-90444C40F7EC}    RtkRecNoLimitApi Class
{8E93A1B1-8EF0-42e9-AC76-D2CA4CF28681}    OptPCEE3Prop Class
{919E321F-A0D6-460d-9333-1A0FAD222AB7}    MaxxVolumeSDAPO Class
{91FE738D-615F-424B-B329-028ACFC193E1}    NSSimpleControl Class
{93EC11E9-889B-458e-8DEE-B750C8AAC6C2}    RtApocapsApi Class
{97D6882F-029B-4CAD-9043-9152A78EFB74}    SoundAliveFMPage Class
{9914A841-B21A-489C-949C-89306F33BF9A}    DSpruseApi Class
{9C4B415C-B076-43F4-928D-98D8B465087A}    DtsS2UltraPcApi Class
{9D1C81FD-A77A-4cc0-BD6E-A827C9E38ACA}    MaxxAudio3Api Class
{9F39C0AE-979D-4BFC-890D-4BDF6FD7BDE1}    DDLiveApi Class
{A20B899B-D65D-4D75-A919-57D94C36DD93}    SRSAPOOpModeEnumerator Class
{A2414C63-45E9-48db-9C94-EB7D28494D08}    SFAPOGFX Class
{A27368B3-D810-42ce-B114-83900258B8EC}    RtkAPOGFX Class
{A296D363-EE83-4af9-9BE7-729C1296150A}    RtkAPOMFX Class
{A29EB043-6CE2-4ee2-B38C-F58719E0D88F}    RtkAPOEFX Class
{A51A19D6-80F1-4abf-AB95-AF5215E8B052}    RtkRecLFX Class
{A5A63314-41AC-484F-85B8-FC15335C24CF}    RtUpDownMixApi Class
{A69C91DC-11C4-414f-A919-4DA8EA3F3CA6}    RtkRecMFX Class
{A6CB57B4-E35B-4ddd-BC32-CA3D4479079D}    DolbySprucePage Class
{A6EDD1A5-1ACA-4110-9B21-AD7EDC210CA3}    RtkRecSFX Class
{AAF1A9FE-267C-4528-ADFE-F34397B99B6D}    MaxxAudioAPO Class
{AB3B404A-B18F-4b4f-B91F-77F2DE95EB18}    RtkRecEFX Class
{ac66b852-e245-11e2-a28f-0800200c9a66}    NSControl Class
{AC86A15E-8043-47BC-AE95-C0466E56F1AF}    DTSAPOIntelDSP Class
{AD7476AF-BE9F-409a-9A66-FFD991FEC6D2}    RtkClrRecPage Class
{AE0B08BE-FF0E-4FF6-BEC5-24BFD96B4050}    Dolby Digital Plus Analog Mainstream Class
{AFA95F79-06AC-4B9A-B261-D415063DC2B3}    SRSTruSurroundXTPropertyPage Class
{B4380351-FA1F-4F54-9831-BA54EA5F8906}    TIPropertyPage Class
```

Page 12

SOFTWARE OUTPUT.txt

```
{B4928187-D2E3-4CFA-A2C2-A9C97B4956EA}   DmsApi Class
{B786AA8A-3748-4cf4-9F64-F4077DA25F0F}   OptPCEE3Prop Class
{BA671804-F70B-4bc4-AB81-FD8CA07ECE62}   SRS_WOWHD Class
{BBA39DEF-B0D8-4D50-9133-85D5B1AC7971}   RtDataProc Class
{BC1F9ACF-DCA1-43d4-AFEE-D742DC11473C}   RtkRecEffectsApi Class
{C26C3384-7112-4b5a-8BB5-1328D9543D79}   SonyApi Class
{C4686FF2-11A2-4e2e-A670-AAF1E8B295B4}   AndreaRenderPage Class
{C51686E8-256E-4bee-9A7A-08A55C48A718}   BbePropPage Class
{C8197EBA-2423-43ed-B9E6-D8C63B928D5A}   DTSU2PPage Class
{CC4F0992-6318-4767-ADF4-892D05E727F5}   SRSCOMEndpointInfo Class
{CE93F536-D2FB-4e8f-8193-F57AD8BC90D5}   DTSPSApi Class
{D030594F-5F74-4517-A61B-D4ADDAF7979C}   TADEFxRender Class
{D4A1C23B-049F-44f6-8CE0-8173614AAC9A}   KnowlesPage Class
{d7296011-e245-11e2-a28f-0800200c9a66}   NAHIMICAPO LFX Class
{d7296012-e245-11e2-a28f-0800200c9a66}   NAHIMICAPO APO GFX Class
{D86A0539-030B-4D8E-8120-46D67250BE14}   SRS_TruSurroundHD4 Class
{D9A965B0-0278-4972-B82E-299F34FC0B54}   SrsPropPage Class
{DA2C9ECE-7418-4906-B4FA-0A00B3EB88AA}   RtkAPOSFX Class
{DC253AB8-10DC-483c-AB5F-D6A4E189FD70}   RtkAPOLFX Class
{DC805502-D8AC-49F9-921C-572C29F86283}   SRSAPOQCDSP Class
{DDCFD625-B4EA-4528-AC09-39D695027AC4}   ConexantPage Class
{DDE20A40-F390-4616-AE98-2BA9E8C70744}   Dolby Digital Plus P Analog Class
{E0760680-E3E3-41A6-A5BE-275F5C21BDD9}   DPCEE3sApi Class
{E4D7C1C8-9459-45f8-A541-CE54DE835DD5}   RtkUtilApi Class
{E51EF0ED-35D5-4bde-93E9-28CA62B1E704}   MDRCApi Class
{E56DE49D-C11A-4C42-B7B2-E7384B2FA40C}   SRSAPOCOMControl Class
{E9A2EE74-9791-4dc6-9066-D7D908C6C613}   DtsS2PropPage Class
{EE4B528E-5C11-4f80-BCA3-C88647061D79}   DTSConnectPage Class
{F2464A7E-5B09-4199-826F-7D6A16AF2E59}   RtkWavesApi Class
{F59167DD-ED87-4f6c-843D-33219D584756}   SrsDisablePage Class
{F5972329-BC50-4B55-9734-830FBF2DED93}   SRS_TruSurroundHD Class
{F69B7E4A-4A83-4485-8860-85DAA196D745}   TSXTBlockPropertyPage Class
{FB6AE33C-D9B6-4b09-8DF1-AE7AAD5C9530}   DolbyPCEE3sPage Class
{FCDE348C-3789-43E4-B80D-BED94FBB02B8}   SRSAPOSystem Class
{FD2EF96F-8896-4b9b-8924-CD915D3F052B}   SFAPOLFX Class
{FF894E2A-5C73-4b58-838B-81958856CFB5}   DtsApoUpcSyBtPage Class
Thu Aug 13 22:28:13 2015 Z
{0066D4B3-8DE0-4D08-AA83-EDD50E2431F0}
Thu Aug 13 22:19:08 2015 Z
{4BE8D3C0-0515-4A37-AD55-E4BAE19AF471}   Intel® Quick Sync Video H.264 Encoder MFT
Thu Aug 13 22:19:07 2015 Z
{071BCD17-1720-430B-AB8B-D6E4AB56689F}   TheIntelSmartFrame Class
{0F0D27EA-8DDE-471A-B786-85B2444E2F55}   DDE Agent class
{113FAE2B-FF38-4054-9229-467410D6EB27}   Intel® AAC encoder
{14E3BDA2-C480-4E09-8C71-A4A7031B341D}   WD Audio Filter
{19E8E555-8374-4DC9-8FED-87C30AA74A52}   WD Silence Filter
{1ABC749F-6FD8-429A-BA11-F3179033C196}   Intel® Mux Properties
{1E719CDE-6B71-40AD-B442-AD02C129B3E2}   WD Secure Source Filter
{241C022B-8D0B-447E-B8A6-525DAED49E4B}   Intel® Mux Renderer
{27E7234F-429F-4787-AC8F-8AADDED01355}   PSFactoryBuffer
{280A8F40-E382-11D2-B561-00A0C92E6848}   Software\Intel\Display\igfxcui
{3B8F6B19-C9CE-4985-B09D-5A781EF85960}   Intel® properties
{45244F59-BE44-45D2-8B67-C8D4FE270EB6}   TheLaunchTimeEnhancer Class
Thu Aug 13 21:54:48 2015 Z
{ED32C084-BABB-11E1-B491-D4D66088709B}   Clearfi Shell Extension
Thu Jul 16 03:40:55 2015 Z
{00B01B2E-B1FE-33A6-AD40-57DE8358DC7D}   System.Security.Cryptography.HMACSHA1
{01FF4E4B-8AD0-3171-8C82-5C2F48B87E3D}
System.Runtime.Remoting.Metadata.SoapMethodAttribute
{026CC6D7-34B2-33D5-B551-CA31EB6CE345}   System.Collections.SortedList
{047A9A40-657E-11D3-8D5B-00104B35E7EF}   Microsoft Common Language Runtime Debugger
Publisher
{05EBA309-0164-11D3-8729-00C04F79ED0D}   Cor IE Security Manager,
```

Page 13

SOFTWARE OUTPUT.txt

```
CorIESecurityManager, CorIESecurityManager 1
    {06B81C12-A5DA-340D-AFF7-FA1453FBC29A}
System.Security.Policy.AllMembershipCondition
    {07F94112-A42E-328B-B508-702EF62BCC29}
System.Runtime.InteropServices.COMException
    {08295C62-7462-3633-B35E-7AE68ACA3948}    System.ObsoleteAttribute
    {09A60795-31C0-3A79-9250-8D93C74FE540}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapInteger
    {0A29FF9E-7F9C-4437-8B11-F424491E3931}    NDP SymBinder
    {0A3976C5-4529-4ef8-B0B0-42EED37082CD}    NDP SymReader
    {0AE2DEB0-F901-478b-BB9F-881EE8066788}    NDP SymWriter
    {0D23F8B4-F2A6-3EFF-9D37-BDF79AC6B440}    System.Reflection.TargetException
    {0D52ABE3-3C93-3D94-A744-AC44850BACCD}
System.Collections.Generic.KeyNotFoundException
    {0E4EFFC0-2387-11D3-B372-00105A98B7CE}    Microsoft.JScript.JSAuthor
    {0E71F9BD-C109-3352-BD60-14F96D56B6F3}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNormalizedString
    {0F424AB8-3D71-3F74-B230-EFB0144788ED}
    {0FF66430-C796-3EE7-902B-166C402CA288}    System.MemberAccessException
    {108296C1-281E-11D3-BD22-0000F80849BD}    Pdb based CorSymWriter
    {112BC2E7-9EF9-3648-AF9E-45C0D4B89929}    System.TypeLoadException
    {11581718-2434-32E3-B559-E86CE9923744}    System.OperationCanceledException
    {1163D0CA-2A02-37C1-BF3F-A9B9E9D49245}
System.Runtime.Remoting.Proxies.ProxyAttribute
    {146855FA-309F-3D0E-BB3E-DF525F30A715}    System.Collections.Hashtable
    {146A47AB-A2CF-3587-BB25-2B286D7566B4}    System.Globalization.NumberFormatInfo
    {14910622-09D4-3B4A-8C1E-9991DBDCC553}    System.Diagnostics.StackFrame
    {14BE6B21-C682-3A3A-8B24-FEE75B4FF8C5}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtokens
    {14D4CBD9-7490-4F25-BAA6-1C5E22F6B1E3}    PimcManager Class
    {1890B385-5DD3-33B4-84DB-24FD1685F33D}
    {18B1C7EE-68E3-35BB-9E40-469A223285F7}
System.Runtime.Serialization.OnDeserializedAttribute
    {1A06A4DC-E239-3717-89E1-D0683F3A5320}    System.Globalization.KoreanCalendar
    {1C97EF1D-74ED-3D21-84A4-8631D959634A}
System.Runtime.Serialization.OptionalFieldAttribute
    {1D2680C9-0E2A-469d-B787-065558BC7D43}    Fusion Cache
    {1E66F26B-79EE-11D2-8710-00C04F79ED0D}    Cor MIME Filter, CorFltr, CorFltr 1
    {1EC2DE53-75CC-11d2-9775-00A0C9B4D50C}    Microsoft Common Language Runtime Meta
Data
    {1F17C39C-99D5-37E0-8E98-8F27044BD50A}
System.Security.Cryptography.DSASignatureDeformatter
    {1F9F18A3-EFC0-3913-84A5-90678A4A9A80}
System.Security.Cryptography.RijndaelManaged
    {20051D1B-321F-3E4D-A3DA-5FBE892F7EC5}    System.Security.Cryptography.HMACRIPEMD160
    {204D5A28-46A0-3F04-BD7C-B5672631E57F}
System.Runtime.InteropServices.PreserveSigAttribute
    {21F5A790-53EA-3D73-86C3-A5BA6CF65FE9}    System.Runtime.Remoting.ObjRef
    {2206D773-CA1C-3258-9456-CEB7706C3710}    System.Globalization.HebrewCalendar
    {24540EBC-316E-35D2-80DB-8A535CAF6A35}    System.Runtime.Remoting.RemotingException
    {24EEC005-3938-3C71-821D-7F68FD850B2D}
System.Runtime.Remoting.Messaging.RemotingSurrogateSelector
    {2763BE6B-F8CF-39D9-A2E8-9E9815C0815E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapIdrefs
    {27E986E1-BAEC-3D48-82E4-14169CA8CECF}
System.Threading.ThreadInterruptedException
    {27F31D55-D6C6-3676-9D42-C40F3A918636}    System.IO.StringWriter
    {2846AE5E-A9FA-36CF-B2D1-6E95596DBDE7}    System.Reflection.AmbiguousMatchException
    {29625281-51CE-3F8A-AC4D-E360CACB92E2}
System.Diagnostics.DebuggerNonUserCodeAttribute
    {29A6CF6F-D663-31A7-9210-1347871681FC}
System.Security.Permissions.GacIdentityPermission
    {29C69707-875F-3678-8F01-283094A2DFB1}    System.CannotUnloadAppDomainException
```

Page 14

SOFTWARE OUTPUT.txt
```
{29C98DFC-AC6B-4788-BDDD-CA41D6D3704A}   Dia based SymReader
{2B4B0612-E1F4-376F-A9B9-86BA3F72A670}
{2BB6C5E0-C2B9-3608-8868-21CFD6DDB91E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNonPositiveInteger
{2C314899-8F99-3041-A49D-2F6AFC0E6296}   System.Security.Cryptography.HMACSHA256
{2D5EC63C-1B3E-3EE4-9052-EB0D0303549C}
System.Runtime.InteropServices.SafeArrayTypeMismatchException
{2DECBCB7-BAC0-316D-9131-43035C5CB480}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDate
{30AC0B94-3BDB-3199-8A5D-ECA0C5458381}
System.Runtime.Serialization.OnDeserializingAttribute
{31C967B5-2F8A-3957-9C6D-34A0731DB36C}   System.Globalization.StringInfo
{31D353B3-0A0A-3986-9B20-3EC4EE90B389}
System.EnterpriseServices.Internal.ServerWebConfig
{346D5B9F-45E1-45C0-AADF-1B7D221E9063}
System.EnterpriseServices.Internal.SoapClientImport
{3495E5FA-2A90-3CA7-B3B5-58736C4441DD}   System.ParamArrayAttribute
{35E946E4-7CDA-3824-8B24-D799A96309AD}   System.Collections.CaseInsensitiveComparer
{36DCDA30-DC3B-4D93-BE42-90B2D74C64E7}
System.EnterpriseServices.RegistrationConfig
{374050DD-6190-3257-8812-8230BF095147}   System.Globalization.JapaneseCalendar
{380BA9E8-E1E6-33C3-8CA9-385FA6E48C88}
{390E92C9-FA66-3357-BEF2-45A1F34186B9}
System.Security.Policy.GacMembershipCondition
{39B68485-6773-3C46-82E9-56D8F0B4570C}   System.Security.Cryptography.MACTripleDES
{3B0398C9-7812-4007-85CB-18C771F2206F}
System.EnterpriseServices.Internal.ComManagedImportUtil
{3BD1F243-9BC4-305D-9B1C-0D10C80329FC}   System.ArgumentNullException
{3C9DCA8B-4410-3143-B801-559553EB6725}   System.Text.UTF7Encoding
{3CDED51A-86B4-39F0-A12A-5D1FDCED6546}
System.Runtime.Remoting.RemotingTimeoutException
{3D367908-928F-3C13-8B93-5E1718820F6D}
System.Security.Cryptography.RIPEMD160Managed
{3DDB2114-9285-30A6-906D-B117640CA927}
System.Security.Policy.ApplicationDirectoryMembershipCondition
{3E5509F0-1FB9-304D-8174-75D6C9AFE5DA}   System.Threading.ThreadStateException
{3E8E0F03-D3FD-3A93-BAE0-C74A6494DBCA}   System.AppDomainSetup
{3F281000-E95A-11d2-886B-00C04F869F04}   Com Call Wrapper Unmarshal Class
{3F4A4283-6A08-3E90-A976-2C2D3BE4EB0B}   System.Reflection.AssemblyNameProxy
{3FA7A1C5-812C-3B56-B957-CB14AF670C09}
System.Security.Cryptography.SignatureDescription
{3FB717AF-9D21-3016-871A-DF817ABDDD51}   System.EventArgs
{3FDCEEC6-B14B-37E2-BB69-ABC7CA0DA22F}   System.ArgumentException
{40031115-09D2-3851-A13F-56930BE48038}
System.Security.Cryptography.RNGCryptoServiceProvider
{405C2D81-315B-3CB0-8442-EF5A38D4C3B8}   System.Diagnostics.StackTrace
{40AE2088-CE00-33AD-9320-5D201CB46FC9}
System.Diagnostics.SymbolStore.SymDocumentType
{41970D73-92F6-36D9-874D-3BD0762A0D6F}   System.Diagnostics.DebuggerHiddenAttribute
{4224AC84-9B11-3561-8923-C893CA77ACBE}   System.SystemException
{4286FA72-A2FA-3245-8751-D4206070A191}   System.OverflowException
{432D76CE-8C9E-4EED-ADDD-91737F27A8CB}   Microsoft.JScript.DebugConvert
{433CA926-9887-3541-89CC-5D74D0259144}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapIdref
{43CD41AD-3B78-3531-9031-3059E0AA64EB}   System.Version
{44181B13-AE94-3CFB-81D1-37DB59145030}   System.Security.Cryptography.SHA256Managed
{4479C009-4CC3-39A2-8F92-DFCDF034F748}
System.IO.IsolatedStorage.IsolatedStorageException
{458AA3B5-265A-4B75-BC05-9BEA4630CF18}
System.EnterpriseServices.Internal.AssemblyLocator
{4599202D-460F-3FB7-8A1C-C2CC6ED6C7C8}   System.Collections.Stack
{46080CA7-7CB8-3A55-A72E-8E50ECA4D4FC}
System.Runtime.CompilerServices.CallConvThiscall
```
Page 15

SOFTWARE OUTPUT.txt

```
{463AE13F-C7E5-357E-A41C-DF8762FFF85C}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapMonthDay
   {46E97093-B2EC-3787-A9A5-470D1A27417C}   System.DllNotFoundException
   {475E398F-8AFA-43A7-A3BE-F4EF8D6787C9}
System.Runtime.InteropServices.RegistrationServices
   {477A7D8E-8D26-3959-88F6-F6AB7E7F50CF}   System.Security.Cryptography.HMACSHA512
   {47D3C68D-7D85-3227-A9E7-88451D6BADFC}
System.Collections.CaseInsensitiveHashCodeProvider
   {48728B3F-F7D9-36C1-B3E7-8BF2E63CE1B3}
System.Runtime.Remoting.Channels.TransportHeaders
   {48A75519-CB7A-3D18-B91E-BE62EE842A3E}
System.Threading.SynchronizationLockException
   {48AD62E8-BD40-37F4-8FD7-F7A17478A8E6}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDateTime
   {48C6E96F-A2F3-33E7-BA7F-C8F74866760B}   System.IO.FileNotFoundException
   {48D0CFE7-3128-3D2C-A5B5-8C7B82B4AB4F}
System.Runtime.CompilerServices.MethodImplAttribute
   {4B601364-A04B-38BC-BD38-A18E981324CF}
System.Runtime.CompilerServices.CompilerGlobalScopeAttribute
   {4BE89AC3-603D-36B2-AB9B-9C38866F56D5}
System.Runtime.InteropServices.SafeArrayRankMismatchException
   {4C3EBFD5-FC72-33DC-BC37-9953EB25B8D7}   System.AccessViolationException
   {4C69C54F-9824-38CC-8387-A22DC67E0BAB}
System.Security.Cryptography.X509Certificates.X509Certificate
   {4D187AC2-D815-3B7E-BCEA-8E0BBC702F7C}
System.Security.Cryptography.RSAOAEPKeyExchangeDeformatter
   {4D73E9D0-4716-3585-BE8B-7FF800EE5866}
   {4E515531-7A71-3CDD-8078-0A01C85C8F9D}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapName
   {4E77EC8F-51D8-386C-85FE-7DC931B7A8E7}   System.Random
   {4F272C37-F0A8-350C-867B-2C03B2B16B80}
System.Runtime.Serialization.ObjectIDGenerator
   {50369004-DB9A-3A75-BE7A-1D0EF017B9D3}
System.Runtime.Serialization.Formatters.Binary.BinaryFormatter
   {50AAD4C2-61FA-3B1F-8157-5BA3B27AEE61}   System.STAThreadAttribute
   {52968B13-8F33-33DB-B55F-ED57D7D05E8A}
   {53A3C917-BB24-3908-B58B-09ECDA99265F}
System.Runtime.Remoting.InternalRemotingServices
   {54A05253-96FA-4B98-B8FD-9534D7255914}   PSFactoryBuffer
   {54D8502C-527D-43F7-A506-A9DA075E229C}
System.Management.Instrumentation.ManagedCommonProvider
   {5520B6D3-6EC6-3CE7-958B-E69FAF6EFF99}
System.Runtime.Remoting.Contexts.SynchronizationAttribute
   {5610F042-FF1D-36D0-996C-68F7A207D1F0}
System.Security.AllowPartiallyTrustedCallersAttribute
   {57154C7C-EDB2-3BFD-A8BA-924C60913EBF}
System.Runtime.Serialization.SerializationException
   {58897D76-EF6C-327A-93F7-6CD66C424E11}   System.MissingMethodException
   {58D052BC-A3DF-3508-AC95-FF297BDC9F0C}   System.IO.EndOfStreamException
   {590E4A07-DAFC-3BE7-A178-DA349BBA980B}
System.Runtime.CompilerServices.IUnknownConstantAttribute
   {5A18D43E-115B-3B8B-8245-9A06B204B717}
System.Diagnostics.SymbolStore.SymLanguageType
   {5B76534C-3ACC-3D52-AA61-D788B134ABE2}
System.Runtime.Remoting.Metadata.SoapFieldAttribute
   {5C35F099-165E-3225-A3A5-564150EA17F5}
System.Runtime.Remoting.Channels.ServerChannelSinkStack
   {5C3E6CE8-B218-3762-883C-91BC987CDC2D}   System.Globalization.JulianCalendar
   {5CA9971B-2DC3-3BC8-847A-5E6D15CBB16E}   System.IndexOutOfRangeException
   {5F3A0F8D-5EF9-3AD5-94E0-53AFF8BCE960}
System.Security.Cryptography.ToBase64Transform
   {5F9A955F-AA55-4127-A32B-33496AA8A44E}
System.EnterpriseServices.Internal.SoapUtility
```

Page 16

SOFTWARE OUTPUT.txt
```
{61B3E12B-3586-3A58-A497-7ED7C4C794B9}   System.AppDomainUnloadedException
{62545937-20A9-3D0F-B04B-322E854EACB0}   System.Security.Policy.Evidence
{6276916E-8F41-35C7-B1D2-1D289A63BE7C}
{62E92675-CB77-3FC9-8597-1A81A5F18013}
System.Security.Cryptography.RC2CryptoServiceProvider
{630A3EF1-23C6-31FE-9D25-294E3B3E7486}
System.Runtime.InteropServices.ComRegisterFunctionAttribute
{647053C3-1879-34D7-AE57-67015C91FC70}   System.ArithmeticException
{6619A740-8154-43BE-A186-0319578E02DB}   PSFactoryBuffer
{66CE75D4-0334-3CA6-BCA8-CE9AF28A4396}   System.FlagsAttribute
{673DFE75-9F93-304F-ABA8-D2A86BA87D7C}
System.Security.Cryptography.DSACryptoServiceProvider
{676E1164-752C-3A74-8D3F-BCD32A2026D6}   System.ArrayTypeMismatchException
{682D63B8-1692-31BE-88CD-5CB1F79EDB7B}   System.ApplicationException
{6850404F-D7FB-32BD-8328-C94F66E8C1C7}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNonNegativeInteger
{6896B49D-7AFB-34DC-934E-5ADD38EEEE39}   System.Collections.ArrayList
{68F8AEA9-1968-35B9-8A0E-6FDC637A4F8E}   System.Globalization.GregorianCalendar
{6A02951C-B129-4D26-AB92-B9CA19BDCA26}   Microsoft.JScript.COMPropertyInfo
{6C1C243A-2146-3342-8078-AC4BFB9DB4E9}
System.EnterpriseServices.CompensatingResourceManager.ClerkMonitor
{6D75C88D-82A0-3994-A751-3B82F490D22C}
{6F674828-9081-3B45-BC39-791BD84CCF8F}
System.Security.Cryptography.RSAPKCS1SignatureDeformatter
{6F8527BF-5AAD-3236-B639-A05177332EFE}
System.Runtime.Serialization.OnSerializedAttribute
{70A738D1-1BC5-3175-BD42-603E2B82C08B}   System.Globalization.DateTimeFormatInfo
{726BBDF4-6C6D-30F4-B3A0-F14D6AEC08C7}
System.Resources.MissingManifestResourceException
{742AD1FB-B2F0-3681-B4AA-E736A3BCE4E1}
System.Runtime.InteropServices.MarshalDirectiveException
{74BDD0B9-38D7-3FDA-A67E-D404EE684F24}   System.ArgumentOutOfRangeException
{75215200-A2FE-30F6-A34B-8F1A1830358E}   System.UnauthorizedAccessException
{75999EBA-0679-3D43-BDC4-02E4D637F1B1}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapYear
{769B8B68-64F7-3B61-B744-160A9FCC3216}   System.Globalization.TaiwanCalendar
{777F668E-3272-39CD-A8B5-860935A35181}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapToken
{78D22140-40CF-303E-BE96-B3AC0407A34D}
System.Runtime.InteropServices.RuntimeEnvironment
{7AE01D6C-BEE7-38F6-9A86-329D8A917803}
System.Security.SuppressUnmanagedCodeSecurityAttribute
{7AE844F0-ECA8-3F15-AE27-AFA21A2AA6F8}
System.Security.Cryptography.PKCS1MaskGenerationMethod
{7B2801E6-0BC6-4c92-B742-6BE9B01AE874}   DllHostInitializer
{7B769B29-35F0-3BDC-AAE9-E99937F6CDEC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapPositiveInteger
{7B938A6F-77BF-351C-A712-69483C91115D}
System.Reflection.InvalidFilterCriteriaException
{7BC115CD-1EE2-3068-894D-E3D3F7632F40}
System.Security.Cryptography.RSAPKCS1SignatureFormatter
{7E3393AB-2AB2-320B-8F6F-EAB6F5CF2CAF}   System.Security.UnverifiableCodeAttribute
{7E34AB89-0684-3B86-8A0F-E638EB4E6252}   System.NotFiniteNumberException
{7F6BCBE5-EB30-370B-9F1B-92A6265AFEDD}   System.InvalidCastException
{7F71DB2D-1EA0-3CAE-8087-26095F5215E6}   System.NullReferenceException
{7F8C7DC5-D8B4-3758-981F-02AF6B42461A}
System.Security.Cryptography.CryptographicException
{7F976B72-4B71-3858-BEE8-8E3A3189A651}   System.Collections.Queue
{7FD3958D-0A14-3001-8074-0D15EAD7F05C}   System.Security.Cryptography.SHA384Managed
{7FE87A55-1321-3D9F-8FEF-CD2F5E8AB2E9}   System.Threading.Overlapped
{81C5FE01-027C-3E1C-98D5-DA9C9862AA21}   System.Object
{8352E327-B2EC-3331-9998-817EC5CC93B8}
{837A6733-1675-3BC9-BBF8-13889F84DAF4}
```
Page 17

ᢗ

SOFTWARE OUTPUT.txt
```
System.Runtime.CompilerServices.DiscardableAttribute
  {84589833-40D7-36E2-8545-67A92B97C408}    System.Security.HostSecurityManager
  {84F70B6C-D59E-394A-B879-FFCC30DDCAA2}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapLanguage
  {85EB7D1F-7431-3E1E-A26E-EB1D16CB4ABB}
  {8833BC41-DC6B-34B9-A799-682D2554F02F}    System.IO.DirectoryNotFoundException
  {88C8A919-EB24-3CCA-84F7-2EA82BB3F3ED}
System.Runtime.Serialization.SurrogateSelector
  {89A86E7B-C229-4008-9BAA-2F5C8411D7E0}
System.EnterpriseServices.RegistrationHelper
  {89BCC804-53A5-3EB2-A342-6282CC410260}    System.SerializableAttribute
  {89D26277-8408-3FC8-BD44-CF5F0E614C82}    System.Security.Policy.PolicyException
  {8A3FD229-B2A9-347F-93D2-87F3B7F92753}
System.Runtime.InteropServices.ComConversionLossAttribute
  {8C1425C9-A7D3-35CD-8248-928CA52AD49B}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapHexBinary
  {8C40D44A-4EDE-3760-9B61-50255056D3C7}    System.Text.UTF8Encoding
  {8D36569B-14D6-3C3D-B55C-9D02A45BFC3D}    System.MissingFieldException
  {8F45C7FF-1E6E-34C1-A7CC-260985392A05}
System.Runtime.InteropServices.ComUnregisterFunctionAttribute
  {8F6D198C-E66F-3A87-AA3F-F885DD09EA13}
System.Security.Cryptography.DSASignatureFormatter
  {8FD730C1-DD1B-3694-84A1-8CE7159E266B}
System.Runtime.Remoting.Lifetime.LifetimeServices
  {91591469-EFEF-3D63-90F9-88520F0AA1EF}    System.InvalidProgramException
  {9173D971-B142-38A5-8488-D10A9DCF71B0}    System.Threading.ReaderWriterLock
  {91F672A3-6B82-3E04-B2D7-BAC5D6676609}    System.Diagnostics.Debugger
  {92755472-2059-3F96-8938-8AC767B5187B}
System.Security.Cryptography.RSAPKCS1KeyExchangeFormatter
  {92E76A74-2622-3AA9-A3CA-1AE8BD7BC4A8}    System.MethodAccessException
  {93D11DE9-5F6C-354A-A7C5-16CCCA64A9B8}    System.Reflection.ObfuscationAttribute
  {93F551D6-2F9E-301B-BE63-85AEF508CAE0}
System.Diagnostics.DebuggerStepThroughAttribute
  {9546306B-1B68-33AF-80DB-3A9206501515}    System.InvalidOperationException
  {964AA3BD-4B12-3E23-9D7F-99342AFAE812}    System.FormatException
  {96705EE3-F7AB-3E9A-9FB2-AD1D536E901A}    System.ContextStaticAttribute
  {967696C6-354C-4B5C-9CC8-BD9E1C480C77}    PimcSurrogate Class
  {96A058CD-FAF7-386C-85BF-E47F00C81795}    System.Runtime.InteropServices.InAttribute
  {9A3A64F4-8BA5-3DCF-880C-8D3EE06C5538}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapEntities
  {9A944885-EDAF-3A81-A2FF-6A9D5D1ABFC7}
System.Runtime.InteropServices.InvalidOleVariantTypeException
  {9B924EC5-BF13-3A98-8AC0-80877995D403}
System.Runtime.Remoting.Metadata.SoapAttribute
  {9BF86F6E-B0E1-348B-9627-6970672EB3D3}
System.Runtime.Serialization.OnSerializingAttribute
  {9C125A6F-EAE2-3FC1-97A1-C0DCEAB0B5DF}    System.StackOverflowException
  {9C67F424-22DC-3D05-AB36-17EAF95881F2}
System.Runtime.Remoting.Metadata.SoapTypeAttribute
  {9D309F77-4655-372E-84B0-B0FB4030F3B8}
System.Runtime.InteropServices.SetWin32ContextInIDispatchAttribute
  {9DA2F8B8-59F0-3852-B509-0663E3BF643B}    System.MulticastNotSupportedException
  {9E28EF95-9C6F-3A00-B525-36A76178CC9C}    System.Text.ASCIIEncoding
  {9EA60ECA-3DCD-340F-8E95-67845D185999}    System.Security.Cryptography.CryptoConfig
  {A0E2E749-63CE-3651-8F4F-F5F996344C32}
System.Security.Cryptography.RSAOAEPKeyExchangeFormatter
  {A0F5F5DC-337B-38D7-B1A3-FB1B95666BBF}    System.Text.UnicodeEncoding
  {A164C0BF-67AE-3C7E-BC05-BFE24A8CDB62}    System.IO.IOException
  {A1C0A095-DF97-3441-BFC1-C9F194E494DB}    System.Exception
  {A36738B5-FA8F-3316-A929-68099A32B43B}    System.PlatformNotSupportedException
  {A36E4EAF-EA3F-30A6-906D-374BBF7903B1}    System.Runtime.Remoting.Contexts.Context
  {A3A1F076-1FA7-3A26-886D-8841CB45382F}
System.Runtime.CompilerServices.CallConvCdecl
```
Page 18

SOFTWARE OUTPUT.txt

```
{A5448B7A-AA07-3C56-B42B-7D881FA10934}  System.Security.Policy.ApplicationTrust
{A6673C32-3943-3BBB-B476-C09A0EC0BCD6}  System.Security.Cryptography.SHA512Managed
{A7136BDF-B141-3913-9D1C-9BC5AFF21470}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapYearMonth
{A7248EC6-A8A5-3D07-890E-6107F8C247E5}
System.Runtime.InteropServices.InvalidComObjectException
{A7EDDCB5-6043-3988-921C-25E3DEE6322B}  System.Security.Cryptography.HMACMD5
{A8D058C4-D923-3859-9490-D3888FC90439}
System.Runtime.Serialization.Formatters.SoapFault
{A8F03BE3-EDB7-4972-821F-AF6F8EA34884}  WmiSecurityHelper Class
{A8F9F740-70C9-30A7-937C-59785A9BB5A4}  System.IO.DriveNotFoundException
{AA544D41-28CB-11D3-BD22-0000F80849BD}  SymBinder
{AAD4BDD3-81AA-3ABC-B53B-D904D25BC01E}  System.DataMisalignedException
{AB558A90-77EC-3C9A-A7E3-7B2260890A84}
System.EnterpriseServices.CompensatingResourceManager.Compensator
{ACD857DF-E3D9-36DD-A0AD-7D155D326CE8}
{AD326409-BF80-3E0C-BA6F-EE2C33B675A5}  System.EntryPointNotFoundException
{AD664904-FE8A-3217-BBF5-E6AB1D998F5F}
System.Security.Permissions.HostProtectionAttribute
{AE53ED01-CAB4-39CE-854A-8BF544EEEC35}  System.Security.Cryptography.HMACSHA384
{AF60343F-6C7B-3761-839F-0C44E3CA06DA}  System.Security.Cryptography.CspParameters
{AF8C5F8A-9999-3E92-BB41-C5F4955174CD}  System.IO.FileLoadException
{AFAEF10F-1BC4-351F-886A-878A265C1862}  System.Security.Policy.TrustManagerContext
{AFC681CF-E82F-361A-8280-CF4E1F844C3E}
System.Runtime.InteropServices.ExternalException
{AFEF65AD-4577-447A-A148-83ACADD3D4B9}  System.Data.SqlClient.SQLDebugging
{B0F64827-79BB-3163-B1AB-A2EA0E1FDA23}
System.EnterpriseServices.Internal.ComSoapPublishError
{B406AC70-4D7E-3D24-B241-AEAEAC343BD9}  System.MTAThreadAttribute
{B54E38F8-17FF-3D0A-9FF3-5E662DE2055F}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNotation
{B6EB52D5-BB1C-3380-8BCA-345FF43F4B04}
System.Security.Cryptography.DESCryptoServiceProvider
{B71E484D-93ED-4B56-BFB9-CEED5134822B}  Microsoft.JScript.Vsa.VsaEngine
{B81CB5ED-E654-399F-9698-C83C50665786}
System.Runtime.InteropServices.OptionalAttribute
{B81FF171-20F3-11d2-8DCC-00A0C9B00525}  Type name parser and builder
{BC5062B6-79E8-3F19-A87E-F9DAF826960C}
System.Runtime.Remoting.Services.EnterpriseServicesHelper
{BCB67D4D-2096-36BE-974C-A003FC95041B}
System.Runtime.CompilerServices.CallConvStdcall
{BDA7BEE5-85F1-3B66-B610-DDF1D5898006}  System.FieldAccessException
{C016A313-9606-36D3-A823-33EBF5006189}  System.IO.PathTooLongException
{C03880A5-0B5E-39AD-954A-CE0DCBD5EF7D}  System.AppDomainManager
{C1ABB475-F198-39D5-BF8D-330BC7189661}
System.Security.Cryptography.FromBase64Transform
{C30ABD41-7B5A-3D10-A6EF-56862E2979B6}
System.Runtime.Remoting.Messaging.OneWayAttribute
{C41D0B30-A518-3093-A18F-364AF9E71EB7}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNegativeInteger
{C41FA05C-8A7A-3157-8166-4104BB4925BA}
System.Security.Cryptography.CryptographicUnexpectedOperationException
{C498F2D9-A77C-3D4B-A1A5-12CC7B99115D}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtoken
{C5B56EA1-5853-3310-B3E2-924E9F0BA355}
{C76B435D-86C2-30FD-9329-E2603246095C}
System.Runtime.Remoting.Metadata.SoapParameterAttribute
{C7B9C313-2FD4-4384-8571-7ABC08BD17E5}  Microsoft.JScript.COMMethodInfo
{C9F0A842-3CE1-338F-A1D4-6D7BB397BDAA}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDay
{C9F61CBD-287F-3D24-9FEB-2C3F347CF570}  System.RankException
{CA0F511A-FAF2-4942-B9A8-17D5E46514E8}  Microsoft.JScript.COMFieldInfo
{CA35CB3D-0357-11D3-8729-00C04F79ED0D}  Microsoft.IE.Manager
```

Page 19

SOFTWARE OUTPUT.txt

```
{CA805B13-468C-3A22-BF9A-818E97EFA6B7}
System.Runtime.InteropServices.SEHException
    {CAA817CC-0C04-4D22-A05C-2B7E162F4E8F}
System.EnterpriseServices.Internal.SoapServerVRoot
    {CAEC7D4F-0B02-3579-943F-821738EE78CC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapMonth
    {CB2F6723-AB3A-11d2-9C40-00C04FA30A3E}  Microsoft Common Language Runtime Meta
Data
    {CBEAA915-4D2C-3F77-98E8-A258B0FD3CEF}  System.ContextMarshalException
    {CC20C6DF-A054-3F09-A5F5-A3B5A25F4CE6}  System.DuplicateWaitObjectException
    {CC77F5F3-222D-3586-88C3-410477A3B65D}  System.NonSerializedAttribute
    {CCF306AE-33BD-3003-9CCE-DAF5BEFEF611}  System.OutOfMemoryException
    {CDC70043-D56B-3799-B7BD-6113BBCA160A}  System.MissingMemberException
    {CDFA7117-B2A4-3A3F-B393-BC19D44F9749}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapAnyUri
    {CE39D6F3-DAB7-41b3-9F7D-BD1CC4E92399}  WCF/COM+ Integration Service Moniker
    {CF8F7FCF-94FE-3516-90E9-C103156DD2D5}
System.Runtime.Serialization.Formatters.InternalRM
    {D049DC2B-82C3-3350-A1CC-BF69FEE3825E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapTime
    {D13B741D-051F-322F-93AA-1367A3C8AAFB}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNcName
    {D23D2F41-1D69-3E03-A275-32AE381223AC}
System.Runtime.Serialization.FormatterConverter
    {D2548BF2-801A-36AF-8800-1F11FBF54361}
System.Security.Cryptography.MD5CryptoServiceProvider
    {D2EAA715-DAC7-4771-AF5C-931611A1853C}  WmiSinkDemultiplexor Class
    {D41969A6-C394-34B9-BD24-DD408F39F261}
System.Resources.MissingSatelliteAssemblyException
    {D5CB383D-99F4-3C7E-A9C3-85B53661448F}
System.Reflection.CustomAttributeFormatException
    {D6564DE1-6163-3076-A8FB-D301CB439E30}
    {D6D2034D-5F67-30D7-9CC5-452F2C46694F}  System.TypeUnloadedException
    {D74D613D-F27F-311B-A9A3-27EBC63A1A5D}  System.Threading.Mutex
    {D8013EEF-730B-45E2-BA24-874B7242C425}  System.EnterpriseServices.Internal.Publish
    {D8013EF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.IISVirtualRoot
    {D8013FF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.GenerateMetadata
    {D8280A4F-FFED-3E98-8928-9F504A4A3361}
    {D8A4F3EB-E7EC-3620-831A-B052A67C9944}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapQName
    {D9035152-6B1F-33E3-86F4-411CD21CDE0E}
System.Security.Cryptography.RSACryptoServiceProvider
    {DA317BE2-1A0D-37B3-83F2-A0F32787FC67}
System.Reflection.TargetParameterCountException
    {DAA132BF-1170-3D8B-A0EF-E2F55A68A91D}
System.Security.Cryptography.TripleDESCryptoServiceProvider
    {DAFB2462-2A5B-3818-B17E-602984FE1BB0}  System.NotSupportedException
    {DB13821E-9835-3958-8539-1E021399AB6C}  System.Runtime.Remoting.ServerException
    {DC5DA001-7CD4-11D2-8ED9-D8C857F98FE3}  Cor Remote Loader, CorLoad, CorLoad 1
    {DD5856E5-8151-3334-B8E9-07CB152B20A4}
System.Runtime.Remoting.Channels.ClientChannelSinkStack
    {DE47D9CF-0107-3D66-93E9-A8ACB06B4583}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDuration
    {DFD888A7-A6B0-3B1B-985E-4CDAB0E4C17D}
System.Diagnostics.SymbolStore.SymLanguageVendor
    {E2C6779C-B7DE-3311-8A5B-41922461E7C0}
    {E38DA416-8050-3786-8201-46F187C15213}  System.Security.XmlSyntaxException
    {E5CB7A31-7512-11D2-89CE-0080C792E5D8}  Microsoft Common Language Runtime Meta
Data
    {E724B749-18D6-36AB-9F6D-09C36D9C6016}  System.Text.StringBuilder
    {E772BBE6-CB52-3C19-876A-D1BFA2305F4E}
```

Page 20

```
                              SOFTWARE OUTPUT.txt
System.Runtime.Serialization.Formatters.SoapMessage
    {E785DD9D-3F87-3679-BB58-A3A4C80F4256}
    {E786FB32-B659-3D96-94C4-E1A9FC037868}   System.ExecutionEngineException
    {E7D574D5-2E51-3400-9FB6-A058F2D5B8AB}
System.EnterpriseServices.Internal.ClientRemotingConfig
    {E822F35C-DDC2-3FB2-9768-A2AEBCED7C40}
System.Runtime.Remoting.Services.TrackingServices
    {E9148312-A9BF-3A45-BBCA-350967FD78F5}   System.BadImageFormatException
    {E947A0B0-D47F-3AA3-9B77-4624E0F3ACA4}
System.Runtime.CompilerServices.IDispatchConstantAttribute
    {EAA78D4A-20A3-3FDE-AB72-D3D55E3AEFE6}   System.TimeoutException
    {EBAA029C-01C0-32B6-AAE6-FE21ADFC3E5D}   System.Security.VerificationException
    {EC3DAC94-DF80-3017-B381-B13DCED6C4D8}   System.Globalization.ThaiBuddhistCalendar
    {ECABAFD1-7F19-11D2-978E-0000F8757E2A}
System.EnterpriseServices.Internal.ClrObjectFactory
    {ED0BC45C-2438-31A9-BBB6-E2A3B5916419}
System.Runtime.CompilerServices.CallConvFastcall
    {EE832CE3-06CA-33EF-8F01-61C7C218BD7E}   System.Globalization.HijriCalendar
    {EE96F4E1-377E-315C-AEF5-874DC8C7A2AA}
System.Security.Cryptography.RSAPKCS1KeyExchangeDeformatter
    {EEC5DCCA-05DC-4B46-8AF7-2881C1635AEA}
System.ServiceModel.Internal.TransactionBridge
    {EEF05C76-5C98-3685-A69C-6E1A26A7F846}   System.Security.SecurityException
    {EF24F689-14F8-4D92-B4AF-D7B1F0E70FD4}
System.EnterpriseServices.Internal.AppDomainHelper
    {F00CA7A7-4B8D-3F2F-A5F2-CE4A4478B39C}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapEntity
    {F12FDE6A-9394-3C32-8E4D-F3D470947284}   System.Reflection.AssemblyName
    {F1C3BF79-C3E4-11D3-88E7-00902754C43A}
System.Runtime.InteropServices.TypeLibConverter
    {F1EBA909-6621-346D-9CE2-39F266C9D011}
System.Runtime.InteropServices.ComImportAttribute
    {F59D514C-F200-319F-BF3F-9E4E23B2848C}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapBase64Binary
    {F5E692D9-8A87-349D-9657-F96E5799D2F4}   System.IO.MemoryStream
    {F6914A11-D95D-324F-BA0F-39A374625290}   System.DivideByZeroException
    {F6B6768F-F99E-4152-8ED2-0412F78517FB}
System.EnterpriseServices.Internal.SoapServerTlb
    {F8BE2AD5-4E99-3E00-B10E-7C54D31C1C1D}   System.NotImplementedException
    {FA0B54D5-F221-3648-A20C-F67A96F4A207}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapId
    {FC13A7D5-E2B3-37BA-B807-7FA6238284D5}
System.Security.Cryptography.SHA1CryptoServiceProvider
    {FD5CD8B1-6FE0-44F3-BBFB-65E3655B096E}
    {FD8C8FCE-4F85-36B2-B8E8-F5A183654539}
System.Runtime.Remoting.Lifetime.ClientSponsor
    {FDB2DC94-B5A0-3702-AE84-BBFA752ACB36}
System.Runtime.InteropServices.OutAttribute
    {FDF9C30D-CCAB-3E2D-B584-9E24CE8038E3}   System.Security.Cryptography.SHA1Managed
    {FEDB2179-2335-48F1-AA28-5CDA35A2B36D}
    {FFC9F9AE-E87A-3252-8E25-B22423A40065}   System.ThreadStaticAttribute
Thu Jul 16 03:34:32 2015 Z
    {331B60DA-9E90-4DD0-9C84-EAC4E659B61F}   Printer Extension Manager Class
    {854A20FB-2D44-457D-992F-EF13785D2B51}
    {95A24F08-5D9A-46F4-8B35-F9905397C741}   PSFactoryBuffer
Thu Jul 16 03:32:37 2015 Z
    {71F96460-78F3-11d0-A18C-00A0C9118956}   WDM Analog Crossbar
Thu Jul 16 03:32:34 2015 Z
    {047ea9a0-93bb-415f-a1c3-d7aeb3dd5087}
Fri Jul 10 13:19:47 2015 Z
    {0CA545C6-37AD-4A6C-BF92-9F7610067EF5}   HNetCfg.FwOpenPort
    {13639463-00DB-4646-803D-528026140D88}   UpdateCollection Class
    {186dd02c-2dec-41b5-a7d4-b59056fade51}   Portable Devices Automation Factory
                              Page 21
```

SOFTWARE OUTPUT.txt

```
{1fb2a002-4c6c-4de7-85c2-cb8db9a4f728}  Microsoft Disk Quota UI Elevation Helper
{21690A61-3629-4E3B-A72D-BBC8A88DB81F}
{241D7C96-F8BF-4F85-B01F-E2B043341A4B}  Workspaces Center
{26D32566-760A-40A2-AA82-A40366528916}  WUPublishedAppInstallorElevator Class
{289AF617-1CC3-42A6-926C-E6A863F0E3BA}  DLNA Media Servers Data Source
{2C5BC43E-3369-4C33-AB0C-BE9469677AF4}  HNetCfg.FwRule
{304CE942-6E39-40D8-943A-B913C40C9CD4}  HNetCfg.FwMgr
{317E92FC-1679-46FD-A0B5-F08914DD8623}  InstallationAgent Class
{32F1EEA8-D64C-4c24-8247-26E648A1D202}
{4026492F-2F69-46B8-B9BF-5654FC07E423}  Windows Firewall
{46CB32FA-B5CA-8A3A-62CA-A7023C0496C5}  CIEContentAdvisorBroker
{4b360c3c-d284-4384-abcc-ef133e1445da}  CIERegistryHKLMBroker
{4CB43D7F-7EEE-4906-8698-60DA1C38F2FE}  UpdateSession Class
{59347292-B72D-41F2-98C5-E9ACA1B247A2}  FaxCommon Class
{5BAF654A-5A07-4264-A255-9FF54C7151E7}  UpdateDownloader Class
{5bbd58bb-993e-4c17-8af6-3af8e908fca8}  IE Spelling Dictionary Installer Broker
{650503CF-9108-4DDC-A2CE-6C2341E1C582}  WebProxy Class
{698F7D05-37F0-4902-8A63-AEF7D44DC7FC}  PortableWorkspaceLauncher Class
{72C97D74-7C3B-40AE-B77D-ABDB22EBA6FB}  StringCollection Class
{7988B571-EC89-11cf-9C00-00AA00A14F56}  Microsoft Disk Quota
{871C5380-42A0-1069-A2EA-08002B30309D}  Internet Folder
{A3DD4F92-658A-410F-84FD-6FBBBEF2FFFE}  Internet Options
{B019E3BF-E7E5-453C-A2E4-D2C18CA0866F}  FlashBroker
{B2C761C6-29BC-4f19-9251-E6195265BAF1}  Color Management
{B699E5E8-67FF-4177-88B0-3684A3388BFB}  UpdateSearcher Class
{bdb57ff2-79b9-4205-9447-f5fe85f37312}  Internet Explorer Add-on Installer
{C01B9BA0-BEA7-41BA-B604-D0A36F469133}  SystemInformation Class
{C2E88C2F-6F5B-4AAA-894B-55C847AD3A2D}  WindowsUpdateAgentInfo Class
{cee8ccc9-4f6b-4469-a235-5a22869eef03}  PNPX Association Class
{D2E0FE7F-D23E-48E1-93C0-6FA8CC346474}  UpdateInstaller Class
{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}  Color Management
{d63c23c5-53e6-48d5-adda-a385b6bb9c7b}  CIEInetcplRasBroker
{E2B3C97F-6AE1-41AC-817A-F6F92166D7DD}  HNetCfg.FwPolicy2
{E5A040E9-1097-4D24-B89E-3C730036D615}  Set Network Location Class Factory
{EC9846B3-2762-4A6B-A214-6ACB603462D2}  HNetCfg.FwAuthorizedApplication
{ECDB0924-4208-451E-8EE0-373C0956DE16}  ECS
{F2CF5485-4E02-4f68-819C-B92DE9277049}  &Links
{F8D253D9-89A4-4daa-87B6-1168369F0B21}  UpdateServiceManager Class
{F942C606-0914-47AB-BE56-1321B8035096}  Storage Spaces
{FBF23B40-E3F0-101B-8488-00AA003E56F8}  Internet Shortcut
Fri Jul 10 13:14:46 2015 Z
{01171F65-249E-4EEB-81BD-03E1B0FA1873}  RoamDictionary Class
{054AAE20-4BEA-4347-8A35-64A533254A9D}  UIHost Class
{075DB5A6-4C67-4816-AE00-7451EC2AAA51}  NBDocument Class
{07DC68FA-A15D-4E44-93DE-645060C7B469}  HandWritingSkinProps Class
{137f5ec6-cf6b-482f-acea-c687dfbd199d}  Microsoft Input Personalization Plug-in
{14834D34-8CEE-459e-8520-2264EC46E099}  SharedHWProperties Class
{1B9A0947-4903-45FE-9B96-FE0E80C35D9C}
Windows.Devices.Sensors.ActivitySensorTriggerDetails
{1E2D67D6-F596-4640-84F6-CE09D630E983}  ShapeCollector Class
{23571E11-E545-4DD8-A337-B89BF44B10DF}  PSFactoryBuffer
{2853ADD3-F096-4C63-A78F-7FA3EA837FB7}  Input Panel Configuration
{2E1AE5DF-5A6F-420A-9B7B-41E5BA8FA36D}  HWProp Class
{2E483DC9-7E4D-4861-B496-7E00B7FA184F}  NbTextLayoutPageText Class
{3429E395-176B-4a0a-863D-FCA6B19073BA}  GeneralProperties Class
{3529B1D2-313A-4202-BD3E-5996B7E18A10}
{3697C5FA-60DD-4B56-92D4-74A569205C16}  Tablet PC Correction for Windows Journal
{39C42C60-85F5-40ED-BF39-975A0AA0B2A4}  HandWritingSkin Class
{3B68879A-2CE5-419D-BB70-F39E1F66B06F}  MathRecognizer Class
{46445657-1F22-11DA-A2D9-00065B83EE53}  PSFactoryBuffer
{4B0A2997-E555-4F84-B45B-68AB8BC57635}  RdpEndpoint Class
{4CE576FA-83DC-4f88-951C-9D0782B4E376}  UIHostNoLaunch Class
{4FDDEA74-513D-4454-90B4-4AB1011157AD}  Stationery Class
```

Page 22

SOFTWARE OUTPUT.txt

```
{565E978D-AC10-443A-A2C8-165C2DA1B5FC}  Sticky Notes Windows Desktop Search
Protocol Handler
  {56C4F5A2-E217-4610-83CC-89F09E07782B}  NbCompositeLayer Class
  {5828227c-20cf-4408-b73f-73ab70b8849f}  UMRDPProtocolManager  Class
  {5BD3EA21-163B-4B17-951E-E73EEBF0601A}  RotationManager Class
  {5d8539fa-9e3b-459f-8118-020b5ef1796e}  JNT Persistent Handler
  {5ea4f148-308c-46d7-98a9-49041b1dd468}  Mobility Center Control Panel
  {5ED98377-87A3-4d86-81F7-3E46E0342833}
  {6101F767-998E-452B-B54A-E836DD486BAD}  SensorClassExtension Class
  {64445657-9101-11d9-994B-00301BB132BA}  InkItem Class
  {6B19643A-0CD7-4563-B710-BDC191FCAD3B}  TSFstateManager Class
  {70445657-5AB0-11d9-A4E5-00301BB132BA}  InkStore Class
  {74ABD359-DD57-46b2-B459-B8FC803E67D4}  TipSettings Class
  {76DC8129-0A40-45eb-B0DC-09E8C6CDDE9D}  NbTextLayoutPageProp Class
  {77A1C827-FCD2-4689-8915-9D613CC5FA3E}  SensorManager Class
  {79C43ADB-A429-469F-AA39-2F2B74B75937}  SensorCollection Class
  {802B1FB9-056B-4720-B0CC-80D23B71171E}  Microsoft PenInputPanel Control
  {807C1E6C-1D00-453f-B920-B61BB7CDD997}  Microsoft TipAutoCompleteClient Control
  {83FEFA40-6F67-4244-AA04-1E590C1CB1D9}  TextContributor Class
  {85183dd5-755d-4952-aa8f-c02e5c4f0651}  InkAnalyzer
  {8613E14C-D0C0-4161-AC0F-1DD2563286BC}  Correction Widget Class
  {88EEBD3A-9091-44b8-92A7-F0D595422D90}  GesturesProperties Class
  {8A539A30-0653-4E54-91B8-C8CF5DE862A1}  RichInkSegment Class
  {8BA2F157-CC2D-4d7a-BE0B-99C53DB78F10}  NbDocCstg Class
  {8C24BE77-7E9E-4d5c-85F7-EFC393B5FEC4}  NbBaseEditableDocument Class
  {901AB1E6-3EC9-4aae-AEE5-188013A5CC21}  RioEventSender Class
  {9209B7D1-6DA5-43E4-BCD1-F2BE497635E7}  RdpEndpoint Class
  {936812D2-D700-407B-BDF6-D00ACD1CC047}  Custom Sensor Device Access Capability
Handler Plugin
  {9F074EE2-E6E9-4d8a-A047-EB5B5C3C55DA}  HwTextInsertion Class
  {A666634D-333F-4CC9-AF78-65ED7DB1D6C3}  PSFactoryBuffer
  {a81d181b-0fd4-4442-91a1-b6febfaf1dc6}  Journal File Filter Class
  {AFE0D06B-E242-47ea-A987-74EB2D1030E6}  NbTextLayoutPage Class
  {B7A44F26-0114-4285-B4BA-C9E78C4F9416}  NbDocView Class
  {B86BB667-9FEC-4285-A03A-10BC98C1CA1C}
  {BA9FCBAC-3AE4-46BF-B7BA-669498CCC8DE}  CPreferredTIPState Class
  {be472f80-fa9a-46d8-a158-f888836d8e0b}  SystemTouchKeyboard Class
  {C168CDC0-6292-46DF-B34D-29D7580D2CE5}  Emoji MFU Setting Handler
  {C4D6E899-E38A-4838-9188-0B98EE3175E6}  ProgrammabilityManager Class
  {C4D77430-755D-4E19-A6E1-AA8CA5E0E7BC}  TipTsfData Class
  {C561816C-14D8-4090-830C-98D994B21C7B}  MathInputControl Class
  {C6465C2C-7943-452a-9A57-F61DB6B452E9}  TextPrediction Language Model
  {D6E88812-F325-4dc1-BBC7-23076618E58D}  TsfManager Class
  {DCD33DDD-2A79-40D1-8319-864D416440AA}  PSFactoryBuffer
  {E94137E0-92ED-4579-9251-18AF2A08CCD1}  Tablet Tip Soft Keyboard Skin Class
  {EBDD6BF3-AF35-4bf1-9EE3-335A3F5DE0FF}  NbAccessibleObject Class
  {ED834ED6-4B5A-4bfe-8F11-A626DCB6A921}  Personalization Control Panel
  {F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6}  CPenIMX Class
  {f33915da-f694-41db-a87e-a0ad42ee00c3}  Microsoft Input Personalization Plug-in
Setup
  {F3B4F2E9-CCCC-49aa-B0B2-2C4A02E69A37}  TabTipUI Class
  {F3F5824C-AD58-4728-AF59-A1EBE3392799}  Sticky Notes Namespace Extension for
Windows Desktop Search
  {F87CB264-80B7-4df8-9E62-ABC259074CF6}  NbRioEventSink Class
  {F9B189D7-228B-4F2B-8650-B97F59E02C8C}  Microsoft TextInputPanel Object
  {FC138128-D766-4f2a-9EA6-6C88E3EC2301}  NbBitmapLayer Class
  {FD8D7237-49E4-4B99-A580-ACA91ED6FCDA}  RioTabletInput Class
Fri Jul 10 13:12:08 2015 Z
  {61A48126-EF74-4D4A-9DDA-43FD542CAD1E}
  {9DAA54E8-CD95-4107-8E7F-BA3F24732D95}
Fri Jul 10 11:05:55 2015 Z
  {00000507-0000-0010-8000-00AA006D2EA4}  ADODB.Command
  {0000050B-0000-0010-8000-00AA006D2EA4}  ADODB.Parameter
```

Page 23

```
                        SOFTWARE OUTPUT.txt
{00000514-0000-0010-8000-00AA006D2EA4}  ADODB.Connection
{00000535-0000-0010-8000-00AA006D2EA4}  ADODB.Recordset
{00000560-0000-0010-8000-00AA006D2EA4}  ADODB.Record
{00000566-0000-0010-8000-00AA006D2EA4}  ADODB.Stream
{00020810-0000-0000-C000-000000000046}
{00020811-0000-0000-C000-000000000046}
{00020820-0000-0000-C000-000000000046}
{00020821-0000-0000-C000-000000000046}
{00020900-0000-0000-C000-000000000046}
{00020906-0000-0000-C000-000000000046}
{00020D75-0000-0000-C000-000000000046}
{0482DDE0-7817-11CF-8A03-00AA006ECB65}  KsDataTypeHandlerAnalogVideo
{05589F80-C356-11CE-BF01-00AA0055595A}  KsDataTypeHandlerVideo
{083863F1-70DE-11D0-BD40-00A0C911CE86}  ActiveMovie Filter Class Manager
{096CBB6C-221A-4A5D-B609-0C7534E3EE1F}
Windows.Devices.Sms.SmsMessageReceivedTriggerDetails
{099EB73C-FF12-45C5-BF64-F0277733A6E2}  OneDriveCloudManagement
{0A81C8B8-8D73-4D29-9C0F-0DF19C5438FD}  CDP Reference Touch Handler
{0c194cb2-2959-4d14-8964-37fd3e48c32d}
{0C1A0EF4-B44F-4179-BDDD-31C27DE7A6D1}
{0C41D1E6-9D16-41ED-9CDD-D0665039857B}
{0C7FF16C-38E3-11d0-97AB-00C04FC2AD98}  SQLOLEDB
{10072CEC-8CC1-11D1-986E-00A0C955B42E}  PeerDraw Class
{103874F6-2837-4156-9C6A-DEE9D37CF3DE}
{10A59D3A-E15C-44EC-B6C8-950E713DCA7D}
{11962D33-DEDC-457B-8D75-B3DAD1F202B9}  NgcCtnrContainerVector
{13516F23-4A53-4282-A462-CC1571129539}  NgcCtnr PSFactory
{14F3C12D-7712-42CC-B7CC-64D2BB560C43}
{17CCA71B-ECD7-11D0-B908-00A0C9223196}  Generic WDM Filter Proxy
{19003D25-EAB6-47D7-A4E6-D29D893AE4E2}  CDP Reference Remote Text Handler
{1A8766A0-62CE-11CF-A5D6-28DB04C10000}  WDM Streaming Standard Interface Handler
{1BD3AC02-7468-49C8-80CF-A138ECB84317}  NgcCtnrContainer
{1d6f0f8f-857d-4011-9eb2-69776d1916f0}  PSFactoryBuffer
{206490E7-09B5-4C9D-8E54-254B87A5CEAF}  CDPComAppControlSystemHandler
{2206CDB0-19C1-11D1-89E0-00C04FD7A829}  MSDAINITIALIZE Class
{22c6c651-f6ea-46be-bc83-54e83314c67f}  Folder Infotip
{23650F94-13B8-4F39-B2C3-817E6564A756}
{236C9559-ADCE-4736-BF72-BAB34E392196}
{2465E8F5-E0EA-4BFD-B8B8-A3A6BCB485EB}
{264C15AF-C06A-49A8-BC99-885E4E72E715}  CDPComPrimaryAppSession
{266EEE40-6C63-11cf-8A03-00AA006ECB65}  WDM TV Tuner
{266EEE41-6C63-11cf-8A03-00AA006ECB65}  TV Tuner Property Page
{291EE2A7-BFA5-4e9e-A358-C93655556A6C}  VideoProcAmp2 Class
{2981c306-09ea-405d-9d0f-83337827bd35}
{2C1EAB37-9E2A-459A-821F-9C58036CF42D}  KeywordDetectorMsftSidAdapter Class
{2E1DCDFF-AB5C-47B6-AD3B-169E65344720}
{2EC4C88A-9A75-4C36-A07E-419CB0D78B8E}
{33D9A760-90C8-11D0-BD43-00A0C911CE86}
{33D9A761-90C8-11d0-BD43-00A0C911CE86}  ACM Class Manager
{33D9A762-90C8-11d0-BD43-00A0C911CE86}  WaveIn Class Manager
{34212D32-6E9E-11E2-BDA0-6B2B6288709B}  OneDriveCloudSyncPolicyManager
{37998346-3765-45B1-8C66-AA88CA6B20B8}  CDPComDeviceQuery
{3C9EE142-8A59-4813-A633-206E0C95EA23}
{3F4F9726-2972-4DD4-AB7C-D119F36803B0}  Fingerprint Logon Credential
{3FC77A3B-14C6-41B6-ACC5-ED80223D81C4}  OneDriveSettingSyncProvider
{4075B76F-FCDC-43B6-B0B9-5A005B38B335}
{41fd88f7-f295-4d39-91ac-a85f3149a05b}
{4740316D-2BF9-48EB-A48B-F68298E968AB}  {4740316D-2BF9-48EB-A48B-F68298E968AB}
{498A0351-BA2F-46DD-96D9-C19988FEA0C4}
{4A3F2F56-454A-4CC5-9734-BB7D8141AC0A}  Virtual Factory for Languages
Configuration
{4A56AF32-C21F-11DB-96FA-005056C00008}
{4D4628EA-EDB7-45BC-9CDC-C423780D2F0D}  MobileBroadbandAccountWatcherProxy
                        Page 24
```

```
                        SOFTWARE OUTPUT.txt
{4EFE2452-168A-11d1-BC76-00C04FB9453B}  MidiOut Class Manager
{4F0BCB98-A0D4-4371-92A7-EE6968A89E72}
{557C6CBF-CD77-45CF-84E8-8F5A8A331BAD}  CDPComAppControlClient
{55B3A0BD-4D28-42fe-8CFB-FA3EDFF969B8}
{566296fe-e0e8-475f-ba9c-a31ad31620b1}
{5FAFD868-E3A3-42AC-969D-B69BBE9A400C}
{64818D10-4F9B-11CF-86EA-00AA00B929E8}
{64818D11-4F9B-11CF-86EA-00AA00B929E8}
{65A04334-9DD4-4FA2-94DB-A62922B8BA24}
{687529e6-4d36-4336-88ea-94b03d16aa4b}
{6A2E0670-28E4-11D0-A18C-00A0C9118956}  IAMVideoControl
{6C7977F4-DB5B-4977-9A41-C7344CC43DB9}  Fingerprint Unlock Credential
{6CE77FA1-033F-4275-A363-44B04E289AB6}  NgcProCsp
{6CF48EF8-44CD-45d2-8832-A16EA016311B}
{7197647A-7D2B-42E3-B6E2-9BAABBDC8B67}
{71985F4B-1CA1-11D3-9CC8-00C04F7971E0}
{71F96461-78F3-11d0-A18C-00A0C9118956}  Analog Crossbar Property Page
{71F96462-78F3-11d0-A18C-00A0C9118956}  WDM TV Audio
{71F96463-78F3-11d0-A18C-00A0C9118956}  TV Audio Property Page
{71F96464-78F3-11D0-A18C-00A0C9118956}  VideoProcAmp Property Page
{71F96465-78F3-11D0-A18C-00A0C9118956}  CameraControl Property Page
{71F96466-78F3-11D0-A18C-00A0C9118956}  VideoDecoder Property Page
{71F96467-78F3-11D0-A18C-00A0C9118956}  VideoStreamConfig Property Page
{720D4AC0-7533-11D0-A5D6-28DB04C10000}  KsTopologyInfo Class
{73647561-0000-0010-8000-00AA00389B71}  WDM Streaming Standard Data Type Handler
{73978CED-828C-49AB-A403-9ABACDCE1505}  CDPComMessagingClient
{7751F46E-39B2-4b50-A7E3-23EF598ECD85}  Selector Class
{7D22E920-5CA9-4787-8C2B-A6779BD11781}
{7D5F3CBA-03DB-4BE5-B4B3-6DBED19A6833}
{7ED96837-96F0-4812-B211-F13C24117ED3}
{807553E6-5146-11D5-A672-00B0D022E945}
{81E9DD62-78D5-11D2-B47E-006097B3391B}  DVcrControl Property Page
{865ab07b-1c8e-48c0-b9a7-fa6c5ff48f7b}
{877E4351-6FEA-11D0-B863-00AA00A216A1}  Plug In Distributor: IKsClock
{885735DA-EFA7-4042-B9BC-195BDFA8B7E7}  AzureSettingSyncProvider
{89B36EA2-F25D-4185-BE8B-13BC8904F303}  MobileBroadbandNetworkProxy
{8BDCE735-A077-406B-B526-F1465DD4D35C}  PSFactoryBuffer
{90b9bce2-b6db-4fd3-8451-35917ea1081b}  CLSID_SearchMSExecute
{91EF7526-96DB-489D-8F61-53E2B4DC4039}
{942bc614-676c-464e-b384-d3202aaa02da}  INI Property Set Storage Handler
{98de59a0-d175-11cd-a7bd-00006b827d94}  Microsoft Office Persistent Handler
{9B496CE1-811B-11CF-8C77-00AA006B6814}  IAMTimecodeReader
{9BFFC57B-DF4D-48F7-8C61-B3C969839F74}  {9BFFC57B-DF4D-48F7-8C61-B3C969839F74}
{9C24A977-0951-451A-8006-0E49BD28CD5F}
{9CD31617-B303-4F96-8330-2EB173EA4DC6}
{9DAC2C1E-7C5C-40eb-833B-323E85A1CE84}
{A0227FFC-3AA7-4dc3-9FD7-125745C9EAF6}  CameraControl2 Class
{A03CD5F0-3045-11CF-8C44-00AA006B6814}  IAMExtTransport
{A0D76288-0FB2-477A-96F9-F7EFFD7ED5D3}  CDPComMessagingHost
{A2E3074F-6C3D-11D3-B653-00C04F79498E}
{A3F4E2ED-1E53-438D-B26F-A54740C6F0A1}
{A4A1A128-768F-41E0-BF75-E4FDDD701CBA}  PSFactoryBuffer
{A6BA00FE-40E8-477C-B713-C64A14F18ADB}
{A907657F-6FDF-11D0-8EFB-00C04FD912B2}
{AB824EEF-7CF4-4c55-B415-B2D9CD30FE9E}
{AC59432D-8659-48C4-A584-AFEBC920256F}
{ACAA48D5-5C1E-45EB-8AC4-6D84B9F3A58E}  RmsRoamingSecurityFactory
{AD1841CF-0EC5-4b59-ACC4-8329EED299F9}
{AED5B1AA-CB76-41A7-B534-F99D4D6976F2}
{aef771da-f489-423e-bb0f-634ba8b0c56d}
{B2D2142A-9055-4C37-B3FA-EEFDD4C1DC59}
{b52ab030-8ef5-4621-b480-4d20975d1d26}
{B5730A90-1A2C-11CF-8C23-00AA006B6814}  IAMExtDevice
```

Page 25

SOFTWARE OUTPUT.txt

```
{B927879C-95D3-44BE-81C5-D76FC25ED221}
{B9BC2A50-43C3-41AA-A086-5DB14E184BAE}
{B9BC2A50-43C3-41AA-A087-5DB14E184BAE}
{B9BC2A50-43C3-41AA-A092-5DB14E184BAE}
{bb80e1f9-88d9-4f4a-9522-e99b4e796d75}
{BBA922ED-0AB7-40A7-9E69-495984866A23}
{BC29A660-30E3-11D0-9E69-00C04FD7C15B}    WDM Streaming VPE Property Set Interface
Handler
{C03A0FA8-76AC-4e62-B42A-1F8D8186B0F6}
{c04b329e-5823-4415-9c93-ba44688947b0}
{C100BEBC-D33A-4a4b-BF23-BBEF4663D017}
{C100BED0-D33A-4a4b-BF23-BBEF4663D017}
{C100BED3-D33A-4a4b-BF23-BBEF4663D017}
{C100BED4-D33A-4a4b-BF23-BBEF4663D017}
{C100BED7-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDA-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDB-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDC-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDD-D33A-4a4b-BF23-BBEF4663D017}
{C100BEDE-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE1-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE2-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE3-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE5-D33A-4a4b-BF23-BBEF4663D017}
{C100BEE9-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEA-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEB-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEC-D33A-4a4b-BF23-BBEF4663D017}
{C100BEED-D33A-4a4b-BF23-BBEF4663D017}
{C100BEEE-D33A-4a4b-BF23-BBEF4663D017}
{C19CBBED-8E33-4B9B-8F00-B044415E8764}
{C228A457-53F5-4a76-8035-DF2DA33E76C8}
{C28C7795-22F8-467F-BD15-183453C27491}    {C28C7795-22F8-467F-BD15-183453C27491}
{C2DAE44D-C850-425c-B466-D8CBC1469F5D}
{C4C4C4FC-0049-4E2B-98FB-9537F6CE516D}
{C5621364-87CC-4731-8947-929CAE75323E}    PSFactoryBuffer
{C6E13343-30AC-11D0-A18C-00A0C9118956}    IAMVideoCompression
{C6E13344-30AC-11D0-A18C-00A0C9118956}    IAMDroppedFrames
{C6E13350-30AC-11D0-A18C-00A0C9118956}    IAMAnalogVideoDecoder
{C6E13360-30AC-11D0-A18C-00A0C9118956}    IAMVideoProcAmp
{C6E13370-30AC-11D0-A18C-00A0C9118956}    IAMCameraControl
{c8b522cb-5cf3-11ce-ade5-00aa0044773d}    MSDASQL
{CB378271-9E64-4EE1-ABF2-A5EC8512F352}    CDP Reference App Control Handler
{CBD51D89-C22E-4388-A553-FFE638C76E36}
{cc5bbec3-db4a-4bed-828d-08d78ee3e1ed}    JScript Compact Profile (ECMA 327)
{CCB38336-0B46-4153-BF74-6EA9A8C07EDF}
{D4514024-95CA-45A5-B7B4-A38768D31513}    {D4514024-95CA-45A5-B7B4-A38768D31513}
{D6886603-9D2F-4EB2-B667-1971041FA96B}    NGC Credential Provider
{D6ABE021-1DE0-49F4-895D-E9694D28F0A4}    CRoamingSecurityFactory
{D6FCA954-F7AE-4EAC-8783-85F5E4ABD840}    PSFactoryBuffer
{D8BD090D-3F39-45FD-B29A-7FC62C2E59C3}    ExtTransport2 Class
{DA4E3DA0-D07D-11d0-BD50-00A0C911CE86}    ActiveMovie Filter Categories
{DAB26424-5F5C-4834-8685-A4DB44DF8083}    CDPComGamepadHandler
{DDB93701-527B-4250-B619-672EFD3C5B21}    OneDriveCloudStorageInfo
{DF4FCC34-067A-4E0A-8352-4A1A5095346E}
{dfc8bdc0-e378-11d0-9b30-0080c7e9fe95}    MSDAOSP
{E05592E4-C0B5-11D0-A439-00A0C9223196}    Plug In Distributor: IKsQualityForwarder
{E0F158E1-CB04-11d0-BD4E-00A0C911CE86}    WaveOut and DSound Class Manager
{E1D0AB13-2FE6-4DF0-8917-ED80CF0FEF6B}
{EA7BAE70-FB3B-11CD-A903-00AA00510EA3}
{EA7BAE71-FB3B-11CD-A903-00AA00510EA3}
{EC529B00-1A1F-11D1-BAD9-00609744111A}    WDM Streaming VPE VBI Property Set
Interface Handler
```

Page 26

```
                        SOFTWARE OUTPUT.txt
{ECE71064-011D-45b7-AEF2-3B626985E937}   CPropertyObject Class
{F0183006-8A05-4180-846E-0A8452F6CA40}   {F0183006-8A05-4180-846E-0A8452F6CA40}
{f07f3920-7b8c-11cf-9be8-00aa004b9986}   Microsoft office Filter
{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}   JScript Language
{f414c261-6ac0-11cf-b6d1-00aa00bbbb58}   JScript Language Authoring
{f414c262-6ac0-11cf-b6d1-00aa00bbbb58}   JScript Language Encoding
{F48B770A-CBE5-44C2-8D4F-931DE9CEE6FA}
{F72A76A0-EB0A-11D0-ACE4-0000C0CC16BA}   KsDataTypeHandlerVideo2
{F72A76E0-EB0A-11D0-ACE4-0000C0CC16BA}   KsDataTypeHandlerVBI
{F7DD51E6-1CA0-4A76-B503-F96E0E64CA91}   {F7DD51E6-1CA0-4A76-B503-F96E0E64CA91}
{F827EC16-664E-4B05-878C-02D242229094}
{FAE3D380-FEA4-4623-8C75-C6B61110B681}
{FDD10506-9AE7-4C7D-A407-C109DDEA1845}   Windows.UI.Core.TextInput
{FE67FBE0-B834-4424-880A-52D6F71BA90B}   PSFactoryBuffer
Fri Jul 10 11:05:05 2015 Z
  CLSID  {0000031A-0000-0000-C000-000000000046}
{0000002F-0000-0000-C000-000000000046}   CLSID_RecordInfo
{00000300-0000-0000-C000-000000000046}   StdOleLink
{00000301-A8F2-4877-BA0A-FD2B6645FB94}   PSFactoryBuffer
{00000303-0000-0000-C000-000000000046}   FileMoniker
{00000304-0000-0000-C000-000000000046}   ItemMoniker
{00000305-0000-0000-C000-000000000046}   AntiMoniker
{00000306-0000-0000-C000-000000000046}   PointerMoniker
{00000308-0000-0000-C000-000000000046}   PackagerMoniker
{00000309-0000-0000-C000-000000000046}   CompositeMoniker
{0000030B-0000-0000-C000-000000000046}   DfMarshal
{00000315-0000-0000-C000-000000000046}   Picture (Metafile)
{00000316-0000-0000-C000-000000000046}   Picture (Device Independent Bitmap)
{00000319-0000-0000-C000-000000000046}   Picture (Enhanced Metafile)
{0000031A-0000-0000-C000-000000000046}   ClassMoniker
{0000031D-0000-0000-C000-000000000046}   DCOMAccessControl
{00000320-0000-0000-C000-000000000046}   PSFactoryBuffer
{00000327-0000-0000-C000-000000000046}   objref
{0000032E-0000-0000-C000-000000000046}   PipePSFactory
{0000051A-0000-0010-8000-00AA006D2EA4}   ADO 6.0
{00000541-0000-0010-8000-00AA006D2EA4}   ADODB.Error
{00000542-0000-0010-8000-00AA006D2EA4}   ADODB Error Lookup Service
{00000602-0000-0010-8000-00AA006D2EA4}   ADOX.Catalog.6.0
{00000609-0000-0010-8000-00AA006D2EA4}   ADOX.Table.6.0
{00000615-0000-0010-8000-00AA006D2EA4}   ADOX.Group.6.0
{00000618-0000-0010-8000-00AA006D2EA4}   ADOX.User.6.0
{0000061B-0000-0010-8000-00AA006D2EA4}   ADOX.Column.6.0
{0000061E-0000-0010-8000-00AA006D2EA4}   ADOX.Index.6.0
{00000621-0000-0010-8000-00AA006D2EA4}   ADOX.Key.6.0
{00020000-0000-0000-C000-000000000046}   Microsoft AVI Files
{00020001-0000-0000-C000-000000000046}   AVI Compressed Stream
{00020003-0000-0000-C000-000000000046}   Microsoft Wave File
{0002000D-0000-0000-C000-000000000046}   IAVIStream & IAVIFile Proxy
{0002000F-0000-0000-C000-000000000046}   ACM Compressed Audio Stream
{00020420-0000-0000-C000-000000000046}   PSDispatch
{00020421-0000-0000-C000-000000000046}   PSEnumVariant
{00020422-0000-0000-C000-000000000046}   PSTypeInfo
{00020423-0000-0000-C000-000000000046}   PSTypeLib
{00020424-0000-0000-C000-000000000046}   PSOAInterface
{00020425-0000-0000-C000-000000000046}   PSTypeComp
{00020C01-0000-0000-C000-000000000046}   Sound (OLE2)
{00021400-0000-0000-C000-000000000046}   Desktop
{00021401-0000-0000-C000-000000000046}   Shortcut
{00022601-0000-0000-C000-000000000046}   Media Clip
{00022602-0000-0000-C000-000000000046}   Video Clip
{00022603-0000-0000-C000-000000000046}   MIDI Sequence
{0002DF01-0000-0000-C000-000000000046}   Internet Explorer(Ver 1.0)
{0002DF02-0000-0000-C000-000000000046}   BrowserBroker Class
```

Page 27

SOFTWARE OUTPUT.txt
```
{0002E005-0000-0000-C000-000000000046}   Component Categories Manager
{0002E006-0000-0000-C000-000000000046}   Component Categories Manager with Class
Store
{0003000A-0000-0000-C000-000000000046}   Bitmap Image
{0003000C-0000-0000-C000-000000000046}
{0003000D-0000-0000-C000-000000000046}   Sound
{0003000E-0000-0000-C000-000000000046}   Media Clip
{000C101C-0000-0000-C000-000000000046}   Msi install server
{000C101D-0000-0000-C000-000000000046}   Microsoft Windows Installer Message RPC
{000C103E-0000-0000-C000-000000000046}   PSFactoryBuffer
{000C1090-0000-0000-C000-000000000046}   Microsoft Windows Installer
{000C1094-0000-0000-C000-000000000046}
{0010668C-0801-4DA6-A4A4-826522B6D28F}
{00108226-EE41-44A2-9E9C-4BE4D5B1D2CD}
{0010890e-8789-413c-adbc-48f5b511b3af}   User Notification
{001DC1E0-0F8C-4720-98DB-39D32A661422}   PolicyManager
{002EB8C6-3D34-4848-9A6D-58E388D55908}   CCellularExternalEventHelper
{003e0278-eca8-4bb8-a256-3689ca1c2600}   Published Items Shell Service Object
{006E61DF-1A43-4F2C-B26F-780BAEA3A92D}
{0070746C-9A38-4236-822A-72CC4E5C8087}   Invert Selection command invocation
{00722F5F-CB8F-44D3-AC27-CC37F76CFE92}   Immersive Hotkey Notification
{0086c339-9c0e-4c09-9a2f-ff3d19a44a18}   PSFactoryBuffer
{0095b496-f121-4256-96a0-09179828cc16}   CImeProductObject_JK Class
{009F3B45-8A6B-4360-B997-B2A009A16402}   HomeGroup Task
{00A77FF7-A514-493e-B721-CDF8CB0F5B59}   Computer Info Advise
{00B8308C-09F2-4c18-A7B0-4594D6B22EFE}   Microsoft WBEM (non)Standard Marshaling
for IwbemObjectSinkEx
{00BB2763-6A77-11D0-A535-00C04FD7D062}   Microsoft AutoComplete
{00BB2764-6A77-11D0-A535-00C04FD7D062}   Microsoft History AutoComplete List
{00BB2765-6A77-11D0-A535-00C04FD7D062}   Microsoft Multiple AutoComplete List
Container
{00C429C0-0BA9-11d2-A484-00C04F8EFB69}   CrBlinds
{00CA399E-4CC0-43D2-902B-CEA3D36DC9E4}   Audio Remote Render Endpoint Plugin Stub
Class
{00da2f99-f2a6-40c2-b770-a920f8e44abc}   Staging ShellFolder for CD Burning
{00eebf57-477d-4084-9921-7ab3c2c9459d}   CD Burn Merged Folder
{00f20eb5-8fd6-4d9d-b75e-36801766c8f1}   PhotoAcqDropTarget
{00f210a1-62f0-438b-9f7e-9618d72a1831}   PhotoAcquireOptionsDialog
{00f24ca0-748f-4e8a-894f-0e0357c6799f}   PhotoProgressDialog
{00f26e02-e9f2-4a9f-9fdd-5a962fb26a98}   PhotoAcquire
{00f29a34-b8a1-482c-bcf8-3ac7b0fe8f62}   PhotoAcqDeviceSelectionDlg
{00f2b433-44e4-4d88-b2b0-2698a0a91dba}   PhotoAcqHWEventHandler
{00F2CE1E-935E-4248-892C-130F32C45CB4}   PSFactoryBuffer
{0102563D-F16D-434d-82A2-37968BD3E31E}   RNWF Extensible Helper Class
{011B3619-FE63-4814-8A84-15A194CE9CE3}   WebDVD Device Segment
{011BE22D-E453-11D1-945A-00C04FB984F9}   WSecEdit Security Manager Class
{0131BE10-2001-4C5F-A9B0-CC88FAB64CE8}
{0134A8B2-3407-4B45-AD25-E9F7C92A80BC}   XblAuthManager
{01458CF0-A1A2-11D1-8F85-00600895E7D5}   Interface Proxy Stub
{0149EEDF-D08F-4142-8D73-D23903D21E90}   XDS Feature Segment
{01575CFE-9A55-4003-A5E1-F38D1EBDCBE1}   MsCtfMonitor task handler
{016fd94e-b02a-4ab8-94c6-149fdab56b8d}   PSFactoryBuffer
{01776DF3-B9AF-4E50-9B1C-56E93116D704}   EditionUpgradeHelper Class
{017F10E3-89E4-49F0-B545-618DE31FD27C}   Language Setting Conflict Resolver
{01822ABA-23F0-4506-9BBC-680F5D6D606C}   CLSID_ContactUserAccountChangeCallback
{018f2d58-f16d-448a-bd87-225c8c5d5c94}
{019f7150-e6db-11d0-83c3-00c04fddb82e}   Microsoft IME (Japanese) IFEDict
{01A3BF5C-CC93-4C12-A4C3-09B0BBE7F63F}
{01afc156-f2eb-4c1c-a722-8550417d396f}   Security and Maintenance PSFactory
{01B90D9A-8209-47F7-9C52-E1244BF50CED}
{01CBCF66-A9CA-4449-84DE-7F321232BBC7}   html persistent handler for mapi email
{01D0A625-782D-4777-8D4E-547E6457FAD5}   CEIPLuaElevationHelper
{01E04581-4EEE-11d0-BFE9-00AA005B4383}   &Address
```
Page 28

SOFTWARE OUTPUT.txt

```
{01F36CE2-0907-4d8b-979D-F151BE91C883}    CFrameRateConvertDmo
{01F3E95C-7D8F-46e6-A408-9BA5D1FA5067}    Alpha Listener XML
{01FA60A0-BBFF-11D0-8825-00A0C903B83C}    Encode CRL Distribution Points Class
{01fe4a1f-cc5c-44ab-a1e6-cfbd9249146d}    PSFactoryBuffer
{021003e9-aac0-4975-979f-14b5d4e717f8}    LocalCopyHelper
{021812bc-ae59-4f3c-9e04-72adc0ac9da5}    Per Monitor Shell Positioner Manager
{022BA4BE-26C9-495B-8829-1CDD5946720C}    Device Element Source
{023A36FC-E9D5-419E-824A-CDC66A116E84}    Windows Firewall with Advanced Security
{0245858B-948D-4f36-A574-1A71EF5111CB}
{025A5937-A6BE-4686-A844-36FE4BEC8B6D}    Power Options
{02665D88-6A3E-4DFC-BEFF-8CA2118A5061}    Theme Setting Change Publisher
{026CE3A3-1908-46AA-1988-9B6C290DBB41}    UniversalVoipPolicy
{0273c57c-6693-4444-b20c-a62a3b185b7e}    Device Display Objects Proxies
{027D3767-28E0-4FFA-98D0-DF67D0CBBE47}    User Tile Validator
{02805F1E-D5AA-415B-82C5-61C033A988A6}
{02844640-E37C-4322-A3B8-4C61A2E58879}
{0289a7c5-91bf-4547-81ae-fec91a89dec5}    Microsoft Windows Remote Shell Host
{02A3586C-D264-40BF-97F7-FE40F7E3A882}    Microsoft Virtual Disk Service Dynamic
Provider
{02C09DB6-F3E3-4C27-970D-17107BF4518E}    InkTransform Class
{02C35120-4924-46EB-BC2B-5FB0DB060948}    ImeDicAPIProxy
{02df6db6-9405-4812-b3f6-500e8615b7af}    Registry Data Driven Command
{02E4CBEF-3B8B-4F42-85B9-2BD7BCEC17EE}
{02E6EC4C-96E4-42E8-B533-336916A0087D}    PSFactoryBuffer
{02E7E69E-E80A-48E3-8B1D-6448C25B1710}    CLSID_SettingContentXmlPropertyStore
{02ECA72E-27DA-40E1-BDB1-4423CE649AD9}    WalletFactory
{02F599D5-9AFC-4794-B677-D1149C7C853C}    Game Controller Virtual Key Shell
Component
{03012959-F4F6-44D7-9D09-DAA087A9DB57}
{03022430-ABC4-11D0-BDE2-00AA001A1953}    PSFactoryBuffer
{031E4825-7B94-4dc3-B131-E946B44C8DD5}    UsersLibraries
{031EE060-67BC-460d-8847-E4A7C5E45A27}    Windows Media Player Rich Preview Handler
{032C35F6-11E2-497B-9D78-6AD0288FBD48}    User Tile Broker
{032EE239-DEB8-436E-9043-A2767D457274}    CLSID_ExtensionListContextMenu
{0340F119-A598-4ed9-B0AC-6F6A12D3E755}    Property Store over folder final
{0344ec28-5339-4124-a186-2e8eef168785}    MFSourceFilter
{0358b920-0ac7-461f-98f4-58e32cd89148}    Wininet Cache task object
{0363215C-3B87-4C3D-8300-FF3FD3E02B91}    Immersive Window Message Service
{0369B4E5-45B6-11D3-B650-00C04F79498E}    BDA Tuning Model Channel Tune Request
{0369B4E6-45B6-11D3-B650-00C04F79498E}    BDA Tuning Model ATSC Channel Tune Request
{036A9790-C153-11D2-9EF7-006008039E37}    Audio Mixer
{037BB880-2613-4F6E-9F84-9574CCA8DEAC}
{037c3380-0855-4e8a-8c80-0aa3f697cd27}    TTLS Interactive UI class
{03837511-098B-11D8-9414-505054503030}    TraceDataProviderCollection
{03837513-098B-11D8-9414-505054503030}    TraceDataProvider
{0383751C-098B-11D8-9414-505054503030}    TraceSession
{03837521-098B-11D8-9414-505054503030}    DataCollectorSet
{03837525-098B-11D8-9414-505054503030}    DataCollectorSetCollection
{03837526-098B-11D8-9414-505054503030}    LegacyDataCollectorSet
{03837527-098B-11D8-9414-505054503030}    LegacyDataCollectorSetCollection
{03837528-098B-11D8-9414-505054503030}    LegacyTraceSession
{03837529-098B-11D8-9414-505054503030}    LegacyTraceSessionCollection
{03837530-098B-11D8-9414-505054503030}    TraceSessionCollection
{03837531-098B-11D8-9414-505054503030}    ServerDataCollectorSet
{03837532-098B-11D8-9414-505054503030}    ServerDataCollectorSetCollection
{03837538-098B-11D8-9414-505054503030}    BootTraceSession
{03837539-098B-11D8-9414-505054503030}    BootTraceSessionCollection
{03837546-098B-11D8-9414-505054503030}    ServerDataCollectorSet
{03837547-098B-11D8-9414-505054503030}    SystemDataCollectorSetCollection
{03A84965-6E86-49C5-B831-826B38732363}    PSFactoryBuffer
{03b5835f-f03c-411b-9ce2-aa23e1171e36}    IMJPTIP
{03C036F1-A186-11D0-824A-00AA005B4383}    Microsoft Shell Folder AutoComplete List
{03C06416-D127-407A-AB4C-FDD279ABBE5D}    BDA Tuning Model Digital Cable Locator
```

Page 29

SOFTWARE OUTPUT.txt

```
{03ca8927-0bf5-4df6-9534-0f5e17851944}   CImeDictAPILocalWordComment Class
{03ca98d6-ff5d-49b8-abc6-03dd84127020}   Background Intelligent Transfer Control
Class 2.5
{03e15b2e-cca6-451c-8fb0-1e2ee37a27dd}   CTapiLuaLib Class
{03E7DAD7-17A6-4F91-A879-F276B6FD62F8}   DelegatorProvider
{0413965e-17f3-46b2-b39f-f8aced04194c}   System Setting Applist Sync Handler
{0429EC6E-1144-4bed-B88B-2FB9899A4A3D}   Custom Composition Segment from Data
Services to XDS
{042dc17c-023f-43df-a3ec-982b4dc78a64}   Schema Migration Plugin
{04731B67-D933-450a-90E6-4ACD2E9408FE}   CLSID_SearchFolder
{04788120-12C2-498D-83C1-A7D92E677AC6}   WBEM Framework Instance Provider CIMA
{047DEC5A-95C1-4C86-827F-7B8C92EBA67A}   PSFactoryBuffer
{047FC311-D163-4BF4-8B25-8005623C37DA}   Input Personalization Setting Handler
Callback
{0482E074-C5B7-101A-82E0-08002B36A333}
{049F2CE6-D996-4721-897A-DB15CE9EB73D}   Iris
{04a1e553-fe36-4fde-865e-344194e69424}   Microsoft InkPicture Control
{04A578B2-E778-422A-A805-B3EE54D90BD9}   PSFactoryBuffer
{04A7F8A1-F465-4079-A4FD-B8F4700DF426}   Key Change Provider Monitor
{04B55BC3-33DE-4d79-94EC-830CDF96CC82}   WMPlayer ContentPropPage Class
{04FBCBF4-DC23-3CEC-9025-9D4093C26733}
{05058F23-20BE-11d2-8F18-0000F87A4335}   CLSID_POSyncServices
{0520af9e-e3da-4b32-8be8-0f3e475bfc5f}   Device Center Print Status Extension
{05238C14-A6E1-11D0-9A84-00C04FD8DBF7}   PSFactoryBuffer
{05300401-BCBC-11d0-85E3-00C04FD85AB4}   MHTML Asynchronous Pluggable Protocol
Handler
{05589FA1-C356-11CE-BF01-00AA0055595A}   ActiveMovieControl Object
{05589FAF-C356-11CE-BF01-00AA0055595A}   Audio Renderer Property Page
{055CB2D7-2969-45CD-914B-76890722F112}   BDA Tuning Model MPEG2 Component Class
(Broadcast Substream)
{055E80CA-DD63-4C25-93AB-448BBDB7AA17}   OOBE Region Wizard UI Module
{056440FD-8568-48e7-A632-72157243B55B}   Explorer Navigation Bar
{057EEE47-2572-4AA1-88D7-60CE2149E33C}   PSFactoryBuffer
{05827933-6FB3-4485-89F2-75615F94AAEA}   CLSID_AppSpace
{05A47EBB-8BF0-4CBF-AD2F-3B71D75866F5}   Microsoft H264 Video Remux (MPEG2TSToMP4)
MFT
{05BDC38E-5493-487a-A7FF-8CF2246ABC13}   IE Background Task Scheduler
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d7}   Taskbar Control Panel
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d8}
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d9}   Taskbar
{05DF8D13-C355-47f4-A11E-851B338CEFB8}   CQueryAllWinSAT Class
{05F3561D-0358-4687-8ACD-A34D24C488DF}   Health Center Control Panel
{05f6fe1a-ecef-11d0-aae7-00c04fc9b304}   IntDitherer Class
{05FDB3A2-5639-4D24-AF7D-4C6FB0684661}   DesktopStoreRemediationHandler
{060AF76C-68DD-11D0-8FC1-00C04FD9189D}   Seeking
{06210E88-01F5-11D1-B512-0080C781C384}   PSFactoryBuffer
{06254B9D-05E9-4FBE-968D-F46DBDC91AF9}   MTF Bing AutoSuggestion DS
{06290BD0-48AA-11D2-8432-006008C3FBFC}   Object under which scriptlets may be
created
{06290BD1-48AA-11D2-8432-006008C3FBFC}   Constructor that allows hosts better
control creating scriptlets
{06290BD2-48AA-11D2-8432-006008C3FBFC}   Factory bindable using IPersistMoniker
{06290BD3-48AA-11D2-8432-006008C3FBFC}   Moniker to a Windows Script Component
{06290BD4-48AA-11D2-8432-006008C3FBFC}   Object for encoding scriptlets
{06290BD5-48AA-11D2-8432-006008C3FBFC}   Object for constructing type libraries for
scriptlets
{06290BD8-48AA-11D2-8432-006008C3FBFC}   Constructor for Scriptlet Automation
Handler
{06290BD9-48AA-11D2-8432-006008C3FBFC}   Constructor for Scriptlet Event Handler
{06290BDA-48AA-11D2-8432-006008C3FBFC}   Constructor for Scriptlet ASP Handler
{06290BDB-48AA-11D2-8432-006008C3FBFC}   Constructor for Scriptlet Behavior Handler
{06334b1f-d73e-42f5-a448-5bd2df3c5ec7}   EAPSIM Identity Task class
{063B79F5-7539-11D2-9773-00A0C9B4D50C}   Microsoft COM+ Services Meta Data
```

Page 30

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {063B79F6-7539-11D2-9773-00A0C9B4D50C} | Microsoft COM+ Services Meta Data |
| {06405088-BC01-4E08-B392-5303E75090C8} | Alternates Class |
| {065377f7-9876-4d5a-9f2a-1b4721255a67} | By value marshaled conflict interrupt |
| {0655E396-25D0-11D3-9C26-00C04F8EF87C} | SpLexicon Class |
| {06587E71-F043-403A-BF49-CB591BA6E103} | AudioVolume Class |
| {06622D85-6856-4460-8DE1-A81921B41C4B} | COpenControlPanel |
| {066D2323-D35A-4C15-AE22-F88F136C1613} | KeystrokeGenerator Class |
| {067B4B81-B1EC-489f-B111-940EBDC44EBE} | WMDM CE Device Service Provider |
| {068a8476-9229-4cc0-9d49-2fc699dcd30a} | LPCM MFT |
| {06993B16-A5C7-47EB-B61C-B1CB7EE600AC} | Create and edit Wired policies |
| {06A03425-C9EB-11d2-8CAA-0080C739E3E0} | Help Collection Wrapper Class |
| {06B2132B-5B99-42A6-B8B6-A1709E191C70} | Audio StreamGroup Class |
| {06B32AEE-77DA-484B-973B-5D64F47201B0} | VMR Mixer |
| {06BF8E77-0FEC-4bd3-AFD6-C949AE21E34B} | NarratorToolBar Class |
| {06C792F8-6212-4F39-BF70-E8C0AC965C23} | User Account Control Settings |
| {06CCA63E-9941-441B-B004-39F999ADA412} | MMEndpointManager class |
| {06EEE695-542D-46F6-AEAB-FA2F1B2102D3} | GameCleanupHandler Class |
| {06EEE834-461C-42c2-8DCF-1502B527B1F9} | URL Shortcut PropSetStorage Mapping |
| {0700F42F-EEE3-443a-9899-166F16286796} | HomeGroup Network |
| {0709BCEE-E071-4CF1-BD15-BAEC9AA12D75} | ChxUserDictDS |
| {07252659-bb6b-4b79-b78b-623f6699a579} | AudioConstrictor Class |
| {0725C3CB-FEFB-11D0-99F9-00C04FC2F8EC} | WDM Event Provider |
| {07398dcf-2e0b-4ece-99dd-56b262db948b} | Search Protocol URL Generator |
| {076C2A6C-F78F-4C46-A723-3583E70876EA} | |
| {078759d3-423b-48ad-ab6a-5638c2884dbe} | Shell Undo Parent Unit |
| {079AA557-4A18-424A-8EEE-E39F0A8D41B9} | SAX XML Reader |
| {07A774A0-6047-11D1-BA20-006097D2898E} | Logagent Class |
| {07AA0886-CC8D-4e19-A410-1C75AF686E62} | Onex  PLAP Credential Provider |
| {07B0E5E9-D635-4CD3-B98D-7C10E700DEA0} | PimcSurrogate Class |
| {07B65360-C445-11CE-AFDE-00AA006C14F4} | MIDI Renderer |
| {07C45BB1-4A8C-4642-A1F5-237E7215FF66} | IE Microsoft BrowserBand |
| {07D26616-6136-11D1-8C9C-00C04FC3261D} | |
| {07fc2b94-5285-417e-8ac3-c2ce5240b0fa} | |
| {07FFDD7A-0300-4FDC-B113-1C5364E61F54} | CFeedbackPane |
| {080d0d78-f421-11d0-a36e-00c04fb950dc} | ADs LDAP Pathname Descriptor Object |
| {0814BEF4-2971-429A-B694-2F3E63912DCF} | NarratorExplorerWindow Class |
| {08165EA0-E946-11CF-9C87-00AA005127ED} | WebCheckWebCrawler |
| {08229782-89C8-4028-BB74-75BB58EF1488} | IP Security Monitor |
| {082C78E1-CD8F-4982-BEB9-BBFE43A0F09A} | InkObject Class |
| {0839CA75-2FE4-4608-A1B9-2224E046D6A3} | Modern IME CHT Editing Model |
| {08586F78-3B1F-4CDE-9E87-AFFA015B5DE2} | Windows.System.Profile.SystemManufacturers |

Proxy

| | |
|---|---|
| {08762EA6-B6EF-45FB-B0A5-2F940A849E12} | Backup Restore Services |
| {087798c4-3c0a-48d4-abc9-ed60912fa139} | |
| {0886dae5-13ba-49d6-a6ef-d0922e502d96} | Retail Demo User COM Agent |
| {088714E2-5783-44A2-8552-C9D7E7513339} | DeviceSettingsProvider |
| {088e3905-0323-4b02-9826-5d99428e115f} | |
| {088E8DFB-2464-4C21-BAD2-F0AA6DB5D4BC} | SmartScreen Settings Check Provider |
| {08a99e2f-6d6d-4b80-af5a-baf2bcbe4cb9} | Provides |

IPortableDevicePropVariantCollection helper methods for portable devices
applications and drivers

| | |
|---|---|
| {08d450b7-f7e5-4424-8229-11888adb7c14} | |
| {08d5bfbf-fbca-4322-9f70-ca9f66f8ed6a} | CommonLayoutModifier |
| {08D9DFDF-C6F7-404A-A20F-66EEC0A609CD} | lfsvc |
| {08DFCEF6-4F00-436F-B621-B1585343C2FB} | OOBE OEMRegistration Plugin |
| {08E4F995-1FB3-4705-AC33-6A2B83E9B5BB} | PSFactoryBuffer |
| {08F91D9D-1F00-48C2-B90F-CC75FFAFE727} | SettingSyncParameters |
| {08FC06E4-C6B5-40BE-97B0-B80F943C615B} | Proximity Sharing |
| {08fedb70-9d27-4bcf-bbb0-99986ae2bcb5} | PSFactoryBuffer |
| {09017262-fdb4-4ff2-9013-26332c926ee7} | Csc Sync |
| {09144FD6-BB29-11DB-96F1-005056C00008} | PBDA DTFilter |
| {09290C14-40BF-40F1-A245-85FC671B5FA3} | AboveLockApplicationFrameworkProxy |
| {093FF999-1EA0-4079-9525-9614C3504B74} | Windows Script Host Network Object |

Page 31

SOFTWARE OUTPUT.txt

```
{09474572-B2FB-11D1-A1A1-0000F875B132}   MMCListPadInfo class
{0947c622-f98a-48a5-9df7-60e5fe202e07}   Hide Selected Explorer Command
{0955AC62-BF2E-4CBA-A2B9-A63F772D46CF}   BDA Tuning Model MPEG2 Tune Request
{09655E95-040C-4654-85AF-48852407FDD9}   RADCApiWorkspaceManager Class
{0968e258-16c7-4dba-aa86-462dd61e31a3}   PersistentZoneIdentifier
{0977EEC5-10F7-44AE-A7FA-D4824EBA5C74}   PrintersCacheManager Class
{09799AFB-AD67-11d1-ABCD-00C04FC30936}   Open With Context Menu Handler
{098870b6-39ea-480b-b8b5-dd0167c4db59}   IE OpenService Manager
{098f2470-bae0-11cd-b579-08002b30bfeb}   Null persistent handler
{0997898B-0713-11d2-A4AA-00C04F8EEB3E}   Common Places FS Folder
{09a28848-0e97-4cef-b950-cea037161155}   Remove Properties Drop Target
{09AA621D-CF81-408D-9C9F-41399065CAC4}   Physical Keyboard Skin Class
{09c5dd34-009d-40fa-bcb9-0165ad0c15d4}   User Tile Store
{09DBBC77-588F-4517-A485-74A29759F54C}   PSFactoryBuffer
{09f209a1-d04d-4225-9333-076d72a7bb06}   IPlayToReceiverAppRegistrar Factory
{0A14D3FF-EC53-450f-AA30-FFBC55BE26A2}   TokenActivation Class
{0A16D195-6F47-4964-9287-9F4BAB6D9827}   PSFactoryBuffer
{0A235AB7-264B-4D1A-B533-DD7AB44AD94E}   LiveRegionChangedEvent Class
{0A29F9BD-86B3-4384-B25D-EF1FFE020266}   WSD Scan Proxy
{0A30F902-8398-4ee8-86F7-4CFB589F04D1}   Sync root make available online verb
{0A4B5474-4226-4D28-B4FC-369CC68A7211}   Tablet Mode Positioner
{0A4B8F34-D725-454D-B81D-3BEBE48382DC}
{0A522732-A626-11D0-8D60-00C04FD6202B}   CLSID_CExchImport
{0A556D98-CFEE-4D84-82A7-00377F939198}   Default Associations Profile Handler
{0A56CD6C-B45A-4A6C-A88C-3F42AC7BCED4}   KeyStrokeMonitor Class
{0A6C76BD-9A96-4FD9-930B-F60AF68F6388}   RASGCW Auto Trigger Control Page Class
{0A77F7E3-36D2-4D32-83A8-496A4680C706}
{0A860B80-3773-4DDE-85B4-E68C520A858C}   SpSapiServer Class
{0A886F29-465A-4aea-8B8E-BE926BFAE83E}   EapQecMessenger
{0A88C858-7D0C-4549-9499-7DB05F0CB0BF}   Share Home Group
{0A9AE910-85C0-11D0-BD42-00A0C911CE86}   AVI mux Property Page1
{0a9bbb1e-03ee-4201-9900-abbff56c9c6c}   View Remote Printers Command
{0AA02E8D-F851-4CB0-9F64-BBA9BE7A983D}   AlchemyVis Class
{0AC71593-60FC-4a6a-BF85-A0B93BCC3785}   OOBE TimeDate Plugin
{0AD67D92-C11B-419A-AA28-9045B4169097}   Windows.Management.Provisioning.ProxyStub
{0ADD8D9B-E3C3-43B5-BBCE-1E158E027A64}   CLSID_HtmlDocForParsingSiteUnmarshaller
{0af10cec-2ecd-4b92-9581-34f6ae0637f3}   Provides methods to enumerate and get
information on portable devices and services using IPortableDeviceManager and
IPortableDeviceServiceManager
{0af96ede-aebf-41ed-a1c8-cf7a685505b6}   Library Folder Context Menu
{0AFACED1-E828-11D1-9187-B532F1E9575D}   Folder Shortcut
{0AFCCBA6-BF90-4A4E-8482-0AC960981F5B}
{0B124F8F-91F0-11D1-B8B5-006008059382}   Installed Apps Enumerator
{0B1C8EE2-4E12-496F-BA37-D7337B90FB4B}   PSFactoryBuffer
{0B2C35D2-C8BC-4470-BFC0-D6BB1235E5CE}   Temporary Files Cleaner
{0b2c9183-c9fa-4c53-ae21-c900b0c39965}   CLSID_StartMenuPathCompleteProvider
{0b2feecb-1577-4fa6-9a29-bd9022ebcf90}   CPPTPDiagHelper Object
{0B30F034-02D5-4E2B-9BB7-A9F6538F4110}
{0B3FFB92-0919-4934-9D5B-619C719D0202}   Broadcast Event Service
{0b4c227f-2394-43ff-ba59-bc762f5c46ea}   Windows.Media
{0B4CD745-723E-4D23-B898-47BECD7F0DEF}   Microsoft VPN Client WMIv2 Provider
{0B4E4ABD-BAAC-4822-83A0-936A676196EE}   Windows Connected Search Protocol Provider
{0B5A2C52-3EB9-470a-96E2-6C6D4570E40F}   VssSnapshotMgmt Class
{0B5A7836-4C16-4560-90B2-0F5DAF6D6D1B}   FormHost Class
{0b6d74fe-ad29-4c92-ac06-f06bc2f238a7}   Microsoft Feeds Request
{0b91a74b-ad7c-4a9d-b563-29eef9167172}   Provides IWpdSerializer helper methods for
portable devices drivers
{0BA2A2AC-A4D5-38CB-AD03-A0D5B6EC4646}
{0BD7E521-4DA6-42D5-81BA-1981B6B94075}   PSFactoryBuffer
{0bdc6fc7-83e3-46a4-bfa0-1bc14dbf8b38}   Logon UI Controller
{0BE35200-8F91-11CE-9DE3-00AA004BB851}   Font Property Page
{0BE35201-8F91-11CE-9DE3-00AA004BB851}   Color Property Page
{0BE35202-8F91-11CE-9DE3-00AA004BB851}   Picture Property Page
```

Page 32

SOFTWARE OUTPUT.txt

```
{0BE35203-8F91-11CE-9DE3-00AA004BB851}    Standard Font
{0BE35204-8F91-11CE-9DE3-00AA004BB851}    Standard Picture
{0BE9F729-A4E0-4BED-9FB3-85F1858143B7}    SSPWorkspace Class
{0BEBFF02-C139-4f43-AE23-333A4E635ECE}    NarratorMenuBar Class
{0bf754aa-c967-445c-ab3d-d8fda9bae7ef}    SlideshowContextMenu
{0BFCF7B7-E7B6-433a-B205-2904FCF040DD}    New Shortcut Wizard Modal
{0bfee0ab-71c3-4ffe-89ef-bd28bef201e7}    PSFactoryBuffer
{0c0b25f5-e762-4004-96cd-00ffc1ecb5bf}    Path Property Control
{0C11C759-23B0-4731-8D48-5FE3EA62051F}    Sync roots Profile Notification Handler
{0c15d503-d017-47ce-9016-7b3f978721cc}    Provides IPortableDeviceValues helper
methods for portable devices applications and drivers
{0C313C67-199B-4e68-884D-D36914E26EDD}    CLSID_PeerGroupInvitationXml
{0C3B05FB-3498-40C3-9C03-4B22D735550C}    RasDlg LUA
{0c449b17-06f4-4f1f-a1bf-8cd17fe5d45b}    IMECMDPREDICT
{0C5672F9-3EDC-4b24-95B5-A6C54C0B79AD}    Rational Class
{0C7EFBDE-0303-4c6f-A4F7-31FA2BE5E397}    AlphaImageLoader
{0c9281f9-6da1-4006-8729-de6e6b61581c}    Windows Push Notification Platform
{0c9ac398-8c78-4b4b-b8c6-675ed1b734a1}    IP Route Helper Class
{0CA2640D-5B9C-4c59-A5FB-2DA61A7437CF}    Sync root make available online verb
{0CD397F8-20A2-46F0-BAE8-952DEEEDA2C5}    Connected Account State Change
{0CD7A5C0-9F37-11CE-AE65-08002B2E1262}    Cabinet Shell Folder
{0cdb500e-123f-4e98-b446-0f3eae3c7ebc}    NetBt Helper Class

{0CE7A4A6-03E8-4A60-9D15-282EF32EE7DA}
{0CF32AA1-7571-11D0-93C4-00AA00A3DDEA}    System Monitor Source Properties
{0CF774D0-F077-11D1-B1BC-00C04F86C324}    HTML Host Encode Object
{0CF774D1-F077-11D1-B1BC-00C04F86C324}    ASP Host Encode Object
{0CFAE939-931E-4305-8D05-8C76C254EB34}    MSASR Locale Handler Class (1041)
{0CFDD070-581A-11D2-9EE6-006008039E37}    Generate Black Video
{0D0D66EB-CF74-4164-B52F-08344672DD46}    UPnP Service Provider Class
{0D0E47ED-7220-411f-8F81-1118095DA5E7}    Publication Services Change Data
{0D41EBA2-17EA-4B0D-9172-DBD2AE0CC97A}    SrDrvWuHelper Class
{0D43FE01-F093-11CF-8940-00A0C9054228}    FileSystem Object
{0D45D530-764B-11d0-A1CA-00AA00C16E65}
{0d5c7d36-333d-4f39-9c65-7ab0c48fce32}    Cloud Domain Join AAD Auth Buffer Packager
{0D6417E3-866C-4959-9816-4BF5B85CDAD7}    MsasrUI Class
{0D722F1A-9FCF-4E62-96D8-6DF8F01A26AA}    SpShortcut Class
{0D816B02-D487-44FB-8BD3-7EADB66604CA}    SettingSyncMetadataStore
{0d81ea0d-13bf-44b2-af1c-fcdf6be7927c}    Microsoft DocProp Custom Draw Progress
Control
{0d9b47a2-92b8-4c3b-9147-5b1f1a2e0967}
{0D9D975A-C577-4B5C-93B0-D1BE4944DEDE}
{0da7bfdf-c0a0-44eb-be82-b7a82c4721de}    ARP CBS Uninstaller Proxy
{0DAD2FDD-5FD7-11D3-8F50-00C04F7971E2}    Microsoft ATSC Network Provider
{0DBD7044-8EA5-4573-A924-FE8565CCE18F}    Undo Command
{0DC1AB8B-A52D-4BA8-BD76-E2819386FB2F}    Activation Layout Preferences
{0DD1B55E-2EB8-42E2-B8D0-F11594A29477}    SpStream Class
{0dec7d0c-bd63-4759-aa64-adefd70dcf9a}
{0DED49D5-A8B7-4D5D-97A1-12B0C195874D}    IBDA_PinControl
{0DF44EAA-FF21-4412-828E-260A8728E7F1}    Taskbar
{0DFA72F0-D26C-4987-A128-E3A5641C5568}    CortanaExperienceFlow Class Factory
{0e119e63-267a-4030-8c80-5b1972e0a456}    Shared Memory Stream Marshaller
{0E1487F2-9865-4CD5-B99A-9C5EB063A2BC}    EdgeUI Manager
{0E1EEFB2-E336-481C-B178-36261EC5A843}
{0E21C2A5-88A5-408D-A3F4-480755678C61}    Microsoft Account Device Identity
{0E25DC18-9F5E-48B1-80B3-D124E81B773B}
{0e3be0d7-030e-4ca3-a911-d86e24ae0a3c}    TCImeComponentMgr
{0E41CFB8-0506-40F4-A516-77CC23642D91}    .MF FLAC Media Source ByteStreamHandler
{0E58372A-2CA5-4866-8443-988215E6EE1F}    PSFactoryBuffer
{0E5AAE11-A475-4c5b-AB00-C66DE400274E}    Shell File System Folder
{0E5CBF21-D15F-11D0-8301-00AA005B4383}    &Links
{0E681C52-CD03-11D2-8853-0000F80883E3}
{0e6daa63-dd4e-47ce-bf9d-fdb72ece4a0d}    Device Center Print Context Menu Extension
{0E752416-F29E-4195-A9DD-7F0D4D5A9D71}    Windows Firewall with Advanced Security
```

Page 33

SOFTWARE OUTPUT.txt

```
{0E890F83-5F79-11D1-9043-00C04FD9189D}  DXSurface
{0E94CA61-50B3-4ACD-8276-1A281F3357F3}  Device Element Source View
{0e971350-4039-4a03-85fe-4c210917c26d}  Explorer Settings Monitor
{0E9847B3-13E8-44E6-9659-2B60A140A573}  DM WMI Bridge Provider
{0E9A7BB5-F699-4D66-8A47-B919F5B6A1DB}  ERC Lua Support
{0ea79562-d4f6-47ba-b7f2-1e9b06ba16a4}  AuthBrokerUI
{0EE4845B-96CD-403b-8609-317330581408}  Device Display Status Provider Factory
{0EEA25CC-4362-4a12-850B-86EE61B0D3EB}  Microsoft DocProp Inplace Droplist Combo
Control
{0EEF5FBE-18F3-478A-BD28-4899C2E90323}  SpResourceManager Class
{0f0cf7e2-f98a-4f4a-b684-3bec4b4af892}  PrintTaskConfigurationProxyServer
{0f3ed1f2-afdd-4b0c-b6d9-229c1bc58a08}  IP Path Helper Class
{0F3F9F91-C838-415E-A4F3-3E828CA445E0}  FaxDocument Class
{0F563B5F-8EE2-4516-BA0A-544DE058C75B}  File History staging area cleanup handler
{0F6221DB-8EE7-450D-A28A-2898956004F2}  Mouse Setting Change Publisher
{0F7434B6-59B6-4250-999E-D168D6AE4293}
{0F7650EE-9AFA-47B4-9BE7-F74D9D3C41D7}  Immersive Shell Notifier
{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  TaskScheduler class
{0F92030A-CBFD-4AB8-A164-FF5985547FF6}  SpTextSelectionInformation Class
{0F9FDB2D-1804-4cde-A2F9-9B380CDACF7A}  MtfIHDS
{0fafd998-c8e8-42a1-86d7-7c10c664a415}  Picture Password Enrollment UX
{0FB15084-AF41-11CE-BD2B-204C4F4F5020}  PSFactoryBuffer
{0fb40f0d-1021-4022-8da0-aab0588dfc8b}  UPnPAutomationProxy
{0FC988D4-C935-4b97-A973-46282EA175C8}  PSFactoryBuffer
{0FD19C73-25F5-4A25-B4C5-C77BC26D8E76}  DownloadHandler
{0FE62585-2E14-4bf2-8D61-93954A5F1041}
Fri Jul 10 11:05:04 2015 Z
{0FFD3B05-5194-4e02-A4C8-A1449209F10E}  NarratorThumb Class
{101193C0-0BFE-11D0-AF91-00AA00B67A42}  Display
{101A8FB9-F1B9-11d1-9A56-00C04FA309D4}  CLSID_MessageStore
{102D1D13-BD88-435f-99C1-DE69F1886168}  Credential Page Class
{103E1E59-66D1-4143-B772-8D846E96FEBF}
{104846ab-42b1-4e38-a80d-136f78c3f258}  Browser Progress Aggregator
{10493933-661B-4083-9CE0-EFE48ADD0770}  CLSID_CortanaExperienceMgr
{10898C3A-D2EB-483A-BC44-66BCCF03D6F4}  HidCapabilityHandler
{10BCEB99-FAAC-4080-B2FA-D07CD671EEF2}  IE Recovery Store
{10C1EF5E-6155-4c58-B33B-5D5A78532EE8}  InputEvent Class
{10E2414A-EC59-49D2-BC51-5ADD2C36FEBC}  PSFactoryBuffer
{10E59D21-3860-4ed8-BD52-883E116A892E}  Send Search to Command
{10FEF81C-0DAA-4af0-B714-1F1689C08C8C}  DXVA Allocator
{11016101-E366-4D22-BC06-4ADA335C892B}  IE History and Feeds Shell Data Source for
Windows Search
{1108BE51-F58A-4CDA-BB99-7A0227D11D5E}  Microsoft WBEM _IWmiCallSec Call Security
Factory
{11103421-354C-4CCA-A7A3-1AFF9A5B6701}  MP3 ACM Wrapper MFT
{1123D0C1-886C-42C3-98E6-7109780E8BE2}  IGidsSimulatorManager PSFactory
{11275A82-5E5A-47fd-A01C-3683C12FB196}  MF 3GP Sink Class Factory
{114F5598-0B22-40A0-86A1-C83EA495ADBD}
{1153ACC9-1943-4b3b-B365-0CB8EF9CDE9B}  FocusMonitorPropertyChangeEvent Class
{115e13cf-cfe8-4821-b0da-e06aa4d51426}  RDP Session Agent Class
{11659a23-5884-4d1b-9cf6-67d6f4f90b36}  Ptype_PSFactory
{116ABC1A-F7DB-45A7-ADDA-D5A57A08C6FF}  Workspace Setup Input Page
{116F8D13-101E-4fa5-84D4-FF8279381935}  CompoundCondition Class
{11993195-1244-4840-AB44-480975C4FFE4}  CFileIo
{119b14a0-eb11-40c7-9a3c-e6a8904827d2}  Desktop Retail Demo Idle Detector
{11a25a1d-b9a3-4edd-af83-3b59adbed361}  X509 Endorsement Key
{11d162b6-1cea-4b4a-8037-2518ecd6554b}  CLSID_FTItemContainer
{11D5C91F-0A98-11D1-BB10-00C04FC9A3A3}  Computer Management 1.0 Object
{11D893E6-ED32-4826-BCB1-E5F9E15C4036}  NarratorCommandEvent Class
{11dbb47c-a525-400b-9e80-a54615a090c0}  CLSID_ExecuteFolder
{11F11442-3359-410C-875E-D21984507B62}  Orchestrator Core Service Proxy Stub
{1202DB60-1DAC-42C5-AED5-1ABDD432248E}  Sync Center Client
{1206F5F1-0569-412C-8FEC-3204630DFB70}  Credential Manager
```

Page 34

SOFTWARE OUTPUT.txt
```
{120CED89-3BF4-4173-A132-3CB406CF3231}  DirectSoundParamEqDMO
{122EC645-CD7E-44D8-B186-2C8C20C3B50F}
{12426E70-50E2-3129-B617-E252B36ECE89}
{1249B20C-5DD0-44FE-B0B3-8F92C8E6D080}
{124E2045-8D63-4C23-B420-BBCD6A0ED61A}  Microsoft Network QoS WMI Provider
{12518493-00B2-11d2-9FA5-9E3420524153}  Mounted Volume
{125B0F61-0EC3-4f07-9A49-AFB340D9E57F}  File History Listener CLSID
{1274A710-819D-4AB1-BA5E-27D2D3D27925}  Windows Connected Search History Provider
{127b106b-b42e-4cd8-b08a-22b66a1c7877}  PSFactoryBuffer
{128509e9-c44e-45dc-95e9-c255b8f466a6}  Microsoft FLAC Audio Encoder MFT
{128ACDCE-4D92-4D16-854F-F40AC7311ABB}  CLSID_NotificationController Proxy Stub
{1299CF18-C4F5-4B6A-BB0F-2299F0398E27}  PSFactoryBuffer
{129D7E40-C10D-11D0-AFB9-00AA00B67A42}  DV Muxer
{12C21EA7-2EB8-4B55-9249-AC243DA8C666}  Virtual Factory for DiagCpl
{12D3E372-874B-457D-9FDF-73977778686C}  DeviceIoControl
{12D51199-0DB5-46FE-A120-47A3D7D937CC}  DVD: Pluggable Protocol
{12D73610-A1C9-11D3-BC90-00C04F72DF9F}  SpITNProcessor Class
{12DD4DBB-532B-4FCE-8653-74CDB9C8FE5A}  AudioMixer Class
{12fc5e89-5446-4a7c-ba46-207a29e2945d}  HomeGroup Confirm Page
{130F6206-B21A-4B21-9D98-526B5AECC0BB}  Invoke SettingSync SSO
{1334e551-b2db-429b-a94a-7d6a226ffcbf}
{133eac4f-5891-4d04-bada-d84870380a80}  Shell Create Object Task Server
{13482EC3-06A3-4bb3-84A9-193302B8DD54}
{135698D2-3A37-4d26-99DF-E2BB6AE3AC61}  IVolumeClient3_PSFactory
{135fd325-45b7-4c30-89f8-4386961669f0}  Shell Create Object Handler
{1362ada1-eb60-456a-b6e1-118050db741b}  CertificateAttestationChallenge
{13680CED-AEA0-48d5-A75C-5FD47A3F417A}  LockScreen Tile and Badge Notification
Status Provider
{13709620-C279-11CE-A49E-444553540000}  Shell Automation Service
{1372A97E-2034-41ee-A6C1-1B68FAFA75A1}  CLSID_ICommunityTransport
{13847AF0-912C-470B-87B7-7FC3483BD5F9}
Windows.Security.Authentication.Web.Provider.WebAccountProviderTriggerDetails
{139D8403-E74F-41d2-B103-8790C5C7A517}
{13a4bbe8-6527-40cb-a996-1602829541ef}  Frame Automation Object
{13AA3650-BB6F-11D0-AFB9-00AA00B67A42}  DV Video Encoder
{13B216F4-3CD0-410F-951B-ECED8D7485C6}  NFCProvisioningPlugin
{13B37A2A-546B-47BF-BBCA-8AC97F1EBDCB}  CMpeg2DataControl
{13D3C4B8-B179-4ebb-BF62-F704173E7448}  CLSID_ContactReadingPane
{13DE4A42-8D21-4C8E-BF9C-8F69CB068FCA}  E-Ink
{13F6A0B6-57AF-4BA7-ACAA-614BC89CA9D7}  PSFactoryBuffer
{13F6A0B6-57AF-4BA7-ACAA-614BC89CA9D8}  PSFactoryBuffer
{14010e02-bbbd-41f0-88e3-eda371216584}  CLSID_SearchFolderItemFactory
{14074e0b-7216-4862-96e6-53cada442a56}  Library Icon Extract Extension
{1438B859-8F3B-4053-9C45-EE3D2BAB4611}  NarratorWindow Class
{1438E821-B6D2-11D0-8D86-00C04FD6202B}  CLSID_ApprenticeAcctMgr
{143B03BE-F4B9-4775-979E-5392AB1B7EB2}
{1443904b-34e4-40f6-b30f-6beb81267b80}  cicero sapi layer speech ui server
{144C71F2-7F10-4AB2-BB07-C38F5B9AE05E}  PSFactoryBuffer
{145B4335-FE2A-4927-A040-7C35AD3180EF}  SSDP Provider Class
{14654CA6-5711-491D-B89A-58E571679951}  Microsoft TBAuth Single-Sign On Protocol
{14795a8f-78f3-47bd-acb6-e767414fe293}  Shell Apply Properties Undo Unit
{147A9C5D-36F4-4e3e-BD47-F5F207425085}  HomeGroup Printing Listener Class
{148BD520-A2AB-11CE-B11F-00AA00530503}  Scheduling Agent Task Object Class
{148BD52A-A2AB-11CE-B11F-00AA00530503}  Scheduling Agent Service Class
{14ce31dc-abc2-484c-b061-cf3416aed8ff}  Authentication UI Shutdown Choices
{14d7a407-396b-44b3-be85-5199a0f0f80a}  Media Foundation DShow Source Resolver
{14DD9A1C-7CFF-41be-B1B9-BA1AC6ECB571}  MF AudCap Source Plug-in
{14DE3806-5D5B-405C-AB89-4AC936BCBF48}
{14E1D985-892F-4F52-A866-6B1AE6A53DFE}  NfpService
{14E74C62-DC97-43B0-8F2F-581496A65D60}  SpMMAudioEnum Class
{14FDABF5-AF35-4975-A073-C5017ABDEEAF}  DLNA Content Directory Provider
{150F28F1-49A5-4C28-BE1A-CFA854A1D04B}  TPM Virtual Smart Card VCard Module
Manager
```

Page 35

```
                        SOFTWARE OUTPUT.txt
    {1510FB87-5676-40B9-A227-5D0B66866F81}  PSFactoryBuffer
    {152EA2A8-70DC-4C59-8B2A-32AA3CA0DCAC}  Remote TPM Virtual Smart Card Manager
    {1531d583-8375-4d3f-b5fb-d23bbd169f22}  Windows TXT Previewer
    {1535D95C-2365-447D-9800-B75501A19C0C}  ProtocolForResultsActivatedEventArgs
    {154CF571-B575-4353-A775-D5623728D0F8}  Windows.Devices.WiFi.ProxyStubFactory
    {15756be1-a4ad-449c-b576-df3df0e068d3}  Microsoft DocProp Hyperlink Control
    {1578080A-1AAA-42BD-AA70-254D5452A0AD}
    {15A58581-C545-46FE-BD72-FC6416CD2AF7}  IHVNonUIPage Class
    {15ad6165-baa2-492b-b3cc-e7925d2fab97}  Activation Manager Shim STA
    {15b0bb4c-0f7d-11D1-b21f-00c04Fb9473f}
    {15D6504A-5494-499C-886C-973C9E53B9F1}  BDA Tuning Model DVB Tune Request
    {15deef81-c4c4-431f-b0c9-b62cb9ea3aa9}  Background activation of toast history
changed
    {15E16AEC-F2F0-4E52-B0DF-029D11E58E4B}  MSASR Locale Handler Class (1033)
    {15eae92e-f17a-4431-9f28-805e482dafd4}  Install New Programs
    {15fc1bac-8d83-4e87-8cc2-a70c9f66f943}
    {15FD01A3-6E5D-4ECD-9EBD-1813CB3887A1}  PSFactoryBuffer
    {163FDC20-2ABC-11d0-88F0-00A024AB2DBB}
    {1643E180-90F5-11CE-97D5-00AA0055595A}  Color Space Converter
    {164484A9-35D9-4FB7-9FAB-48273B96AA1D}  RadialWipe
    {1649b154-c794-497a-9b03-f3f0121302f3}  Provides access to a portable device
service using IPortableDeviceService for multi-threaded applications (aggregates the
free-threaded marshaler)
    {1649d1cf-deaf-4a68-abe8-5c9f68572fd1}  ExecuteAssociation
    {165D4642-1278-4486-A3FD-439F5888FCA3}  Workspace Setup Message Page 2
    {16671E5F-0CE6-4CC4-9768-E89FE5018ADE}
    {1677ABA1-4346-442F-A74A-D8B9A713B964}
Windows.Media.Capture.Internal.BroadcastDVRServer.ProxyStubFactory
    {167c0a56-c490-4623-9225-8ffdc546e56c}  Top view restore default command
invocation
    {1685D4AB-A51B-4af1-A4E5-CEE87002431D}  CLSID_GrepProvider
    {168F4281-EC0D-46D3-951D-FBCB2F7C9079}  PSFactoryBuffer
    {1698790a-e2b4-11d0-b0b1-00c04fd8dca6}
    {169A0691-8DF9-11d1-A1C4-00C04FD75D13}  In-pane search
    {16A0A3B9-9F65-4102-9367-2CDA3A4F372A}  AudioFrameNativeFactory
    {16A18E86-7F6E-4C20-AD89-4FFC0DB7A96A}  TPM Virtual Smart Card Manager
    {16AA5514-10D0-47F4-8EFD-FF066D924F2B}  NotificationsSettingsProvider
    {16B280C5-EE70-11D1-9066-00C04FD9189D}  Fade
    {16B280C8-EE70-11D1-9066-00C04FD9189D}  BasicImage
    {16C2C29D-0E5F-45f3-A445-03E03F587B7D}  .group shell context menu
    {16CA098E-5156-4EDC-B064-741AB2B08A38}  Web browser utilities
    {16CA4E03-FE69-4705-BD41-5B7DFC0C95F3}  PSFactoryBuffer
    {16d51579-a30b-4c8b-a276-0ff4dc41e755}  JScript Language
    {16D5A2BE-B1C5-47b3-8EAE-CCBCF452C7E8}  Camera UI Control
    {17072F7B-9ABE-4A74-A261-1EB76B55107A}  WSCProductList Class
    {172BDDF8-CEEA-11D1-8B05-00600806D9B6}  Wbem Scripting Object Path
    {17383A17-6B93-4193-9B60-4D4F99C05163}  SpPhoneticAlphabetConverter Class
    {173FD26E-B0F7-42BF-BFD0-D91DF64CC298}  ITpmVCardManager PSFactory
    {1765E14E-1BD4-462E-B6B1-590BF1262AC6}
    {1767B93A-B021-44EA-920F-863C11F4F768}
    {176961ec-fbfb-4288-b418-c80c86947481}  CVPNDiagHelper Object
    {176D323D-E591-4535-9A09-26F698E5AC5D}  UserLexiconManager Class
    {176d6597-26d3-11d1-b350-080036a75b03}  ICM Scanner Management
    {177C0AFE-900B-48d4-9E4C-57ADD250B3D4}  Microsoft Dolby Digital Plus Decoder MFT
    {179CC917-3A82-40E7-9F8C-2FC8A3D2212B}  SPPLUAObject Class
    {179EE204-246C-4895-919F-5B1D2414B21C}
    {179F3D56-1B0B-42B2-A962-59B7EF59FE1B}  Microsoft TTS Desktop Engine Class -
OneCore
    {17a8b57c-9502-4494-8580-81a9b8069c09}  JScript Diagnostic Component
    {17B001CF-85DA-4D7B-86F9-56119D38692E}  PSFactoryBuffer
    {17B21A1B-6C59-48E0-A448-6BC9AD2C5BFE}
CAppointmentsProviderInternalAddAppointmentActivationPlugin
    {17B75166-928F-417d-9685-64AA135565C1}  Image Transcode
                              Page 36
```

SOFTWARE OUTPUT.txt

```
{17C82257-654E-4C47-8E23-DCA24EAA76A0}   Hybrid Drive Cache Prepopulation Task
{17CCA47D-DAE5-4E4A-AC42-CC54E28F334A}   EditionUpgradeManager Class
{17cd9488-1228-4b2f-88ce-4298e93e0966}   Set User Defaults
{17D6CCD8-3B7B-11D2-B9E0-00C04FD8DBF7}   DsObjectPicker
{17f418ed-5cd0-4067-be51-4c96d386ebc1}   Default Public Save Location verb
{17fb3711-de14-477f-8b81-32a9c11a6938}   CImeCommonAPI Class
{17FC1A80-140E-4290-A64F-4A29A951A867}   OpenMediaSharing
{17FE9752-0B5A-4665-84CD-569794602F5C}
{181A38F4-6CE6-4edc-8DB0-6E5631963A1E}
{181b54fc-380b-4a75-b3f1-4ac45e9605b0}   UPnPDeviceFinderEx Class
{181D6C15-60A6-4BC7-A8E7-389D5BFE4841}   Reading Mode Viewer
{18277AB8-9922-4D26-A4F5-1D10069D106A}   Dual Mode App Open Verb
{182C3813-DF97-40fa-9C4E-B7D3E74F00CA}   Pinned Site Shortcut
{182C40F0-32E4-11D0-818B-00A0C9231C29}   COM+ Catalog Server
{184132B8-32F8-4784-9131-DD7224B23438}
{1860E246-E924-4F73-B2C5-93E0577E3AA1}   IWmiCoreServices Class
{18619969-3835-41E5-B457-44FE0DB77653}   Appx Streaming Data Source Factory
Proxy/Stub Object
{186cda7f-de22-4b95-99b7-49efba0a08f4}   Virtual Desktops
{187463A0-5BB7-11D3-ACBE-0080C75E246E}   WM ASF Reader
{18845040-0fa5-11d1-ba19-00c04fd912d0}   Microsoft HTML Load Options
{18907f3b-9afb-4f87-b764-f9a4e16a21b8}   CLSID_ConditionAttribute
{189255E0-6EF0-41C5-8A1E-3B391D691215}
{18C628EE-962A-11D2-8D08-00A0C9441E20}   Xml2Dex Class
{18E6F425-4735-4DD4-94A0-EB2006451C30}   CLSID_ConnectedSearchErrorService
{18F65133-BB77-4C67-8A64-D427BE942224}
{18FBD4BC-16EA-47f2-8AD0-868C1269C79A}
{1910E202-236A-43E6-9469-FE0B3149F3D9}   Wwan Radio Manager
{19129EAC-A717-4BBD-87E0-615E3C939668}   OOBE HidAccessoryPairing Wizard Page
{19198abd-d4b9-4e14-b156-725f85205f0f}   Full Screen Manager
{19204EDD-187C-40B7-ADA4-79772BD10FB2}   Windows.Devices.SmartCards PSFactory
{19227DC0-FC88-4AAA-8C2D-A0DB913AA2FF}   Snap Component
{19352205-42B0-4690-9AA4-D7DB9AE5F259}   Publication Services Change Data
{193B4137-0480-11D1-97DA-00C04FB9618A}   Microsoft DTC Transaction Unmarshaller
(private, internal)
{1956ED66-CF4D-463A-8C9F-617AD590367D}   NarratorThreadInproc Class
{195B4D07-3DE2-4744-BBF2-D90121AE785B}   Defender CSP
{19603261-6059-43DF-B9E1-8B4352825A90}   scanprofileui class
{1965FEA3-3896-438B-B789-F5981797E7E7}   PSFactoryBuffer
{1968106d-f3b5-44cf-890e-116fcb9ecef1}   Application Registration UI
{196f128d-dce9-4090-b061-3d29c6ca32c2}   Work Offline or Online
{19833350-BF9B-42A1-BDF0-BD1FCBE1FD31}   Immersive TPM Virtual Smart Card Manager
{1992BE97-5290-45A1-897C-4E69431A1803}   CLSID_BackComponentServiceProvider
{19A76FE0-7494-11D0-8816-00A0C903B83C}   Encode String Array Class
{19AD99AE-0DD2-495A-AAC4-015E479722FD}   Virtual Smart Card Manager PSFactory
{19b9dcc7-6f37-4dc7-9da6-8af601c5fce2}   Mobile Broadband Media Manager
{19BA17F2-2602-4E77-9027-103894607626}   Share Media Settings Writer
{19C65143-6230-42FA-A58E-7D9FA9BE2EB5}   WorkspaceBroker Class
{19eb3aee-148e-42fe-a569-a7dc9b25d658}   CMusicPropertiesProxy
{19fb28d1-0e3f-4b94-bd34-8e841aa8b85e}   Windows.Devices.Enumeration Proxy
{1A0391BF-9564-4294-B0A4-06C298929EF9}   Share Specific Users
{1a184871-359e-4f67-aad9-5b9905d62232}   Microsoft Windows Font Context Menu
Handler
{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5}   Sync Center Control
{1A32449E-4C06-4d34-B674-452A952511CE}   MenuOpenedEvent Class
{1A34F5C1-4A5A-46DC-B644-1F4567E7A676}
{1A3F11DC-B514-4B17-8C5F-2154513852F1}
{1A503A1F-BD58-415D-A2FA-A3891F1D99F6}   PSFactoryBuffer
{1A66AEDC-93C3-4ACC-BA96-08F5716429F7}   PSFactoryBuffer
{1a9ca6d5-2488-46b1-b439-218f2314a059}   Desktop Retail Demo Tasks
{1AA9BF05-9A97-48c1-BA28-D9DCE795E93C}   PDF Persistent Handler
{1ab4a8c0-6a0b-11d2-ad49-00c04fa31a86}
{1AB78400-B5A3-4D91-8ACE-33FCD1499BE6}
```

Page 37

SOFTWARE OUTPUT.txt

{1ABB62A5-054D-48A4-9509-D717E39E045B}
Windows.Devices.Perception.ProxyStubFactory
{1AC32B1A-E379-4CAD-B655-F978A30856EC}    GIDS Smart Card Simulator Manager
{1AD699A6-31F7-4EF0-93E9-FFD576F35D30}    OOBE Proxy Wizard Page
{1ADD3454-9CD8-449B-8777-341DAC8A3B0A}    Notification Manager
{1AF81E4E-FC45-48ee-B236-A2A663494390}    Out Of Proc Mapi Handler
{1b00f3f3-945c-4bd3-ade8-77ece2f75dbd}    CloudDomainJoinDataModelServerFactory
{1B02C1F5-555B-4802-96A7-ADDDCCBCA38A}    Wired Network Media Manager
{1B1A897E-FBEE-41CF-8C48-9BF764F62B8B}    SoftKbd Class
{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}    Microsoft WBEM (non)Standard Marshaling
for IEnumWbemClassObject
{1b283861-754f-4022-ad47-a5eaaa618894}    Smartcard Reader Selection Provider
{1B2AFB92-0B5E-4A30-B5CC-353DB4F9E150}    SpSapiServer Class
{1B462D7B-72D8-4544-ACC1-D84E5B9A8A14}    MsRdpSessionManager Class
{1B4DEBEC-0475-4564-B2BF-11490C40AACB}
{1B544C20-FD0B-11CE-8C63-00AA0044B51E}    AVI Splitter
{1B544C24-FD0B-11CE-8C63-00AA0044B520}    DirectX Transform Wrapper Property Page
{1B57B2A1-E763-4676-9064-297F1B413632}    SpMMAudioInLegacy Class
{1B6FC61A-648A-4493-A303-A1A22B543F01}    WSecEdit RSOP Security Settings Class
{1b7cd997-e5ff-4932-a7a6-2a9e636da385}    JScript Language
{1B979846-AAEB-314B-8E63-D44EF1CB9EFC}
System.Diagnostics.DebuggerStepperBoundaryAttribute
{1B9B1983-753C-47ab-9C02-A94EF23154DA}    NarratorSlider Class
{1b9f2bf2-27f5-4dec-a175-3cf7bb8cfd3e}    IP Address Helper Class
{1BA21EC2-FC80-4515-AAAB-F5766A4B88BC}    ConfigUI Class
{1BA783C1-2A30-4ad3-B928-A9A46C604C28}    Create New Link
{1BAC8681-2965-4FFC-92D1-170CA4099E01}    Windows.System.User.ProxyStubFactory
{1BCD547A-62F6-4F2D-A0E3-B4930A3F3C33}    Microsoft Windows Event Tracing Management
WMI Provider
{1BDF02A4-23B7-4173-8107-A56C23124493}    Windows.Graphics.Printing3D.Print3DManager
{1BE1F766-5536-11D1-B726-00C04FB926AF}    EventSystemTier2
{1BE49F30-0E1B-11D3-9D8E-00C04F72D980}    BDA Tuning Model Language Component Type
Class (Broadcast Substream Type)
{1bef2128-2f96-4500-ba7c-098dc0049cb2}    CLSID_DBFolderBoth
{1C0F439D-7C29-4bde-8952-4EEB6A49E048}    CLSID_GrepWdsResolver
{1C15D484-911D-11D2-B632-00C04F79498E}    Legacy Analog TV Tuner Device Segment
{1C16EBAB-7C12-4F21-A2A9-56D67931108F}    Appx HTTPS Streaming Data Source Factory
Object
{1c1800c1-3258-44c2-be80-3deadb6c5e39}    CLSID_KindDescriptionFactory
{1C1EDB47-CE22-4bbb-B608-77B48F83C823}    IE Fade Task
{1c391f2b-801a-416c-9838-6be810293dfc}    Choose Columns Explorer Command
{1C5221CB-C1F6-4999-8936-501C2023E4CD}    Bluetooth FD Provider
{1c5346b8-63e1-4c2b-b125-3c5db94e946c}    TC IME Dictionary Applet
{1C621200-67B2-11D2-9EEB-006008039E37}    Black Generator Property Page
{1C749B87-568C-4865-8E73-6413F8372CE6}    Lpksetup LUA Elevation
{1c773157-69bb-4998-abf1-93a94fd766d3}    CImeDictAPIDictionaryList Class
{1C82EAD9-508E-11D1-8DCF-00C04FB951F9}    Windows Mail Mime Editor
{1c85e599-77dc-416a-ae5d-62569f1872e9}    MediaProcessingTriggerDetails
{1CC6B704-D0F5-4dc3-A521-13620D89E8BC}    Redo Command
{1cc78354-9ded-4c1b-bd81-c67b0289a4e5}    Storage Item Proxy
{1CD0938D-1AC1-49DE-AA04-F2C92D4A02D1}
{1CE75EE1-E27E-4D22-804F-C76D53192D55}    Accessiblity Setting Handler
{1cedc5da-3614-11d2-bf96-00c04fd8d5b0}
{1CF1260C-4DD0-4ebb-811F-33C572699FDE}
{1CF324EC-F905-4c69-851A-DDC8795F71F2}    User Libraries Callback Handler
{1CFC4CDA-1271-11D1-9BD4-00C04FB683FA}    Encode Alternate Name Class
{1D0983EA-B409-44ED-8B61-0406BA1E9C93}    ProxyStubFactory
{1D09B407-A97F-378A-ACCB-82CA0082F9F3}
System.Runtime.Hosting.ApplicationActivator
{1d16438c-54dc-404f-83a9-c041e77a32dd}    DTC Transaction Stats Control
{1D1F0730-0748-4b5f-81DF-865694BD07AC}    IE OrderListExport
{1d27f844-3a1f-4410-85ac-14651078412d}    CompatContextMenu Class
{1d2b8d89-9324-46a0-b797-5725d8c8d881}    SdBackupConfig Class

Page 38

SOFTWARE OUTPUT.txt

```
{1D3529C7-671A-468d-AD2A-499A96B073D1}   AutoConfig Helper Class
{1D428C79-6E2E-4351-A361-C0401A03A0BA}   PSFactoryBuffer
{1D49F57D-47D2-4AEE-A69B-593EC558773F}
{1D5532BB-1E08-4002-8445-8BA35E462045}   HotPlug
{1D583ABC-8A0E-4657-9982-A380CA58FB4B}
{1D6322AD-AA85-4EF5-A828-86D71067D145}   UIAnimationTransitionLibrary
{1d697619-5d35-44a1-a0f6-1c305324c9d0}   InputSwitchControlWrapperClassFactory
{1D858A97-49A3-4805-8390-3BD5976E7ABB}   CLSID_LockScreenApplicationManager
{1d8a9b47-3a28-4ce2-8a4b-bd34e45bceeb}   UPnPDescriptionDocument Class
{1DA08500-9EDC-11CF-BC10-00AA00AC74F6}   VGA 16 color ditherer
{1DCB3A00-33ED-11D3-8470-00C04F79DBC0}   PSFactoryBuffer
{1DF1BDDA-A8FA-4E57-8015-8B621C4DBBE7}
{1DF7D126-4050-47F0-A7CF-4C4CA9241333}   BDA Tuning Model DVB Satellite Locator
{1e0d47e5-a9dc-4998-a572-38c76ef0f5d7}   Media DB Provider Resolver
{1E1714A3-50B9-480b-A94A-636D9A9B56D1}   Shell Indexer Admin Object
{1e46246f-b2ad-4a86-9e08-d0f9e01ee05d}   RetailDemo AppsController
{1E4CEC13-76BD-4ce2-8372-711CB6F10FD1}   XML Paper Specification Filter
{1E54333B-2A00-11d1-8198-0000F87557DB}   DXLUTBuilder
{1E589E9D-8A8D-46d9-A2F9-E6D4F8161EE9}   MF MPEG Property Handler
{1E651CC0-B199-11D0-8212-00C04FC32C45}   Memory Allocator
{1E66C960-3DF9-4d3a-A1A7-CEC25E938C60}   File Placeholder Handler
{1E8F0D70-7399-41BF-8598-7949A2DEC898}   Microsoft DocProp Boolean Control
{1E929228-A702-4239-8780-6DB6D1D83E6B}   Windows.Devices.Printers
{1e94e93c-852d-47fb-9197-7edeb41101b0}   IPHTTPS Helper Class
{1ea1ea14-48f4-4054-ad1a-e8aee10ac805}   Resizer DMO
{1ea5fb56-9ee8-47dc-8998-f45585c2e3e0}   MFPlay Class Factory
{1ecca34c-e88a-44e3-8d6a-8921bde9e452}   Background Intelligent Transfer Control
Class 5.0
{1EE2EAEF-F6FE-4F5B-B9B0-CC6314541025}   ForegroundAppNotificationClient
{1ee7337f-85ac-45e2-a23c-37c753209769}   Smartcard WinRT Provider
{1eeb5b5a-06fb-4732-96b3-975c0194eb39}   Itemsview
{1EF94880-01A8-11D2-A90B-00AA00BF3363}   Microsoft NT DS Class Provider for WBEM
{1f01f4e9-8b75-4e20-8eb0-e49f17f2be61}   Mobile Broadband PromptPinPage Class
{1F046ABF-3202-4DC1-8CB5-3C67617CE1FA}   CLSID_ShowInputPaneAnimationCoordinator
{1F068127-5760-490e-998C-6E35B845F49E}   CLSID_HomeGroupAutoCreateJoin
{1f09b058-f3fd-4a9d-a8ba-a8a05f8fe283}   DTC MMC Property-sheet extension
{1F0BC6AD-46D4-488B-BE1F-047FC7505E60}   ActualWbemAdministrativeLocator Class
{1f1f4e1a-2252-4063-84bb-eee75f8856d5}   WM Speech Encoder DMO
{1f26a602-2b5c-4b63-b8e8-9ea5c1a7dc2e}   SBE2MediaTypeProfile
{1f2e5c40-9550-11ce-99d2-00aa006e086c}   Security Shell Extension
{1f3427c8-5c10-4210-aa03-2ee45287d668}   User Pinned
{1f3d8aa5-9ebf-4ee4-85c2-ea40379aede8}   CScriptedDiag
{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}   Memory Mapped Cache Mgr
{1F5EEC01-1214-4D94-80C5-4BDCD2014DDD}
{1F63F8ED-5DAF-442A-B3A7-8C7B96FB2DD2}   Windows.Management.Lockdown
{1F7D1BE9-7A50-40b6-A605-C4F3696F49C0}   ThirdPartyEapDispatcherPeerConfig
{1f849cce-2546-4b9f-b03e-4004781bdc40}   CLSID_ExplorerLauncher
{1F87137D-0E7C-44d5-8C73-4EFFB68962F2}   Microsoft WMI Provider Subsystem Secured
Host
{1F872270-D68C-4C28-85D9-70CD5FC47A70}   Play all command
{1f9a2c18-d89e-463e-b4f4-bb90152acc64}   MKV Byte Stream Handler
{1FA9085F-25A2-489B-85D4-86326EEDCD87}   Manage Wireless Networks
{1FCE6123-B675-4790-A629-F3E8AC06F839}
{1fda955b-61ff-11da-978c-0008744faab7}   Detection And Sharing
{1fda955c-61ff-11da-978c-0008744faab7}   PSFactoryBuffer
{1FE45ED3-B842-4CF2-8DF6-43E3D6D10E64}   audiokscaptureendpoint class
{1FFDED41-8FC9-497D-BD70-B2E440736273}   Microsoft.WINDOWS.SQLLITE.Engine.4.0
{20076C7E-4851-41ed-9EB8-F4E5F2BB0286}   PSFactoryBuffer
{201600d8-6eff-48ce-b842-e14d37a0682d}   Windows Push Notification Idle Task
Handler
{2025BCB1-370E-4103-9C34-883770F7F2A0}   Package installation state store
enumerator
{203b1eed-db9f-40fb-87bd-1990982017d2}   WMSDK NamespaceFactory Class
```

Page 39

SOFTWARE OUTPUT.txt

```
{20404060-F24F-4F89-84C6-8AF80B0A17CB}   AudioKSRenderEndpoint Class
{20425B74-41F5-426F-A145-13BBB45A2F66}   User OOBE Preparation Plugin
{204810b9-73b2-11d4-bf42-00b0d0118b56}   UPnPRegistrar
{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29}   Microsoft OLE DB Row Position Library
{205447d9-4af1-4f97-a773-e10ff2e44ead}   Immersive Monitor Manager
{20578929-A1F0-4EB1-A4BA-66207291CBA3}   VpnCspv2
{205D7A97-F16D-4691-86EF-F3075DCCA57D}   IE Menu Desk Bar
{205EB05C-A2B9-4135-8645-C8673A7B81F4}   SlideAccessor
{2067ECCC-D717-4b2e-9B39-2847A412F13C}   CLSID_AppSpaceText
{2087c2f4-2cef-4953-a8ab-66779b670495}   WinHttpRequest Component version 5.1
{208D2C60-3AEA-1069-A2D7-08002B30309D}   Network
{209D8461-E6FB-49DD-A824-C9962A9D2F2B}   SpMSSemanticInterpretation Class
{20b1cb23-6968-4eb9-b7d4-a66d00d07cee}   Folder View Host
{20CCEF1E-0185-41a5-A933-509C43B54F98}   ShdocvwBroker
{20cd9315-87d0-40b4-b925-0a8f208e1f8d}   ImeCommonAPI_KOR_Desktop_V1 Class
{20D04FE0-3AEA-1069-A2D8-08002B30309D}   This PC
{20D0DE8D-A98B-4DD4-BA78-612F87EBF890}   Notification Platform Shell Component
{20E25881-F081-448e-85C9-4707A9400593}   User Profile WMI Provider
{20E6D937-F6A7-4C7F-8E69-7E0AF81795FB}   BackgroundTransferPolicy
{20E8B2FE-7568-46AE-A0DB-76B7F469B92D}   About Windows Command
{210DDC43-689C-46E3-BDC1-38C16C8F4C96}   SpObjectTokenEnum Class
{2111CED3-4393-4490-BA09-0714A7C9EA37}   PSFactoryBuffer
{212690FB-83E5-4526-8FD7-74478B7939CD}   Microsoft DTV-DVD Video Decoder
{212BFFFB-DAB9-4EEF-AF58-3366DAAF4C4F}   MCCS SyncActivityFactory
{2135f72a-90b5-4ed3-a7f1-8bb705ac276a}   PicturePasswordLogonProvider
{2155fee3-2419-4373-b102-6843707eb41f}   Local Icon Cache
{215B77BA-853F-48C4-8DC4-024E0D68A812}   SBE Stats - sender side
{2169A933-95E2-41BA-9377-D3FCE9448381}   Windows.Media.Audio
{216C62DF-6D7F-4E9A-8571-05F14EDB766A}   Microsoft DVBT Network Provider
{217700E0-2001-11DF-ADB9-F4CE462D9137}   Provisioning Engine
{217700E0-2003-11DF-ADB9-F4CE462D9137}   Provisioning Refresh Task
{217700E0-2004-11DF-ADB9-F4CE462D9137}   Provisioning Activation Task
{217700E0-2005-11DF-ADB9-F4CE462D9137}   Provisioning Purge Task
{217FC9C0-3AEA-1069-A2DB-08002B30309D}   Shell Copy Hook
{2183DACA-D0BF-4a31-97F7-B87618A81955}   IE Shared Task Scheduler
{21A36DDA-45BD-4F89-881E-0E18FDE90CDF}   PhoneShareObjectProxies
{21AEC8CC-EF8C-422a-8CBC-D3FB3735D855}   NarratorStatusBar Class
{21B22460-3AEA-1069-A2DC-08002B30309D}   File Property Page Extension
{21B82DE4-3BB2-4D10-B382-A614D665F4B5}   Windows Connected Search Zero-Input
Provider
{21D6D48E-A88B-11D0-83DD-00AA003CCABD}   TAPI Class
{21EC2020-3AEA-1069-A2DD-08002B30309D}   All Control Panel Items
{21FE04BD-0FCE-4d3f-A89E-D00CB1421371}   NarratorTogglePattern Class
{2206CDB2-19C1-11D1-89E0-00C04FD7A829}   Microsoft OLE DB Service Component Data
Links
{2206CDB3-19C1-11D1-89E0-00C04FD7A829}   MSDASC Error Lookup
{220898A1-E3F3-46B4-96EA-B0855DC968B6}   Play music command
{220A0D48-03A8-4F7B-8408-4EB506EF68D9}   PSFactoryBuffer
{2227A280-3AEA-1069-A2DE-08002B30309D}   Printers
{2241690B-2E92-46ab-B054-7518558B80DF}   Lock Screen Toast Manager
{2269DAA3-2A9F-4165-A501-CE00A6F7A75B}   Mbn Device Services Manager
{227188db-3179-4fdf-af3a-da3b85a0b3cc}   ImeCommonAPIClassFactory_KOR_Desktop_V1
Class
{227C5B36-F148-4B4B-AEC1-943E394D9885}   Microsoft Windows Firewall WMI Provider
{227ec397-6791-4ac6-a762-2f70f99015c2}   IAS Netsh XML Helper
{228136B0-8BD3-11D0-B4EF-00A0C9138CA4}   Catalog Class
{228136B8-8BD3-11D0-B4EF-00A0C9138CA4}   Cellset Class
{22877a6d-37a1-461a-91b0-dbda5aaebc99}   Recent Places Folder
{228826af-02e1-4226-a9e0-99a855e455a6}   Immersive Shell Broker
{228D9A81-C302-11cf-9AA4-00AA004A5691}   LDAP Provider Object
{228D9A82-C302-11cf-9AA4-00AA004A5691}   LDAP Namespace Object
{2291478C-5EE3-4bef-AB5D-B5FF2CF58352}   MSVidCtl SBE Source to iTV Composition
Segment
```

Page 40

SOFTWARE OUTPUT.txt

```
{2297EF69-AF4B-441D-8F63-4B69C7692DD0}
Windows.Foundation.Diagnostics.ErrorDetails
  {229FC7D6-9056-4e26-A8B9-F546D40200AF}    MCCSAutoDiscover
  {22AF56E3-F2E0-4A7E-AA0C-6B226EF5ABF8}    Work Folders Sync Explorer Status Provider
Class
  {22B6E688-B3A5-44FC-B0CE-69F20653CD61}    Workspace Setup Finish Page
  {22C21F93-7DDB-411C-9B17-C5B7BD064ABC}
  {22C7DA12-F3FD-4875-8344-7786454F6534}    MCCSServerSyncEngine
  {22D6F312-B0F6-11D0-94AB-0080C74C7E95}    Windows Media Player
  {22D8B4F2-F577-4adb-A335-C2AE88416FAB}    PSFactoryBuffer
  {22e5fca2-9c7c-4239-8aed-4d0623f532d8}    CMigrationPlugin Object
  {22EE26E5-2289-11d2-8F43-00C04FC2E0C7}
  {22F1B05B-F983-4CC7-A5F6-67BC2701E29A}    SyncSettingsProvider
  {22f5b1df-7d7a-4d21-97f8-c21aefba859c}    ApplicationLicenseManager
  {22ff30d1-a59e-4580-9190-da3042ceca64}    Mobile Broadband Roaming Page Class
  {233664b0-0367-11cf-abc4-02608c9e7553}    ADS Namespaces Object
  {233A9694-667E-11d1-9DFB-006097D50408}    Windows Mail Address Book
  {23448CEA-DD83-4DC9-AD1C-0E2A70454A3B}
  {235DF164-7970-4B68-8453-2CACFFDD23C9}    MtfIHDSBicount
  {23613363-0028-431D-A49E-A3CD482D3926}    Start Menu Group PolicyFilter
  {23B77E99-5C2D-482D-A795-62CA3AE5B673}    WBEM IP Route Provider
  {23C1F3CF-C110-4512-ACA9-7B6174ECE888}    DsmRefreshTask Class
  {23CF860E-9D2C-451A-8E83-C79C848D85A6}    PSFactoryBuffer
  {23E26328-3928-40F2-95E5-93CAD69016EB}    ZigZag
  {23F24B2D-516C-4E49-B81D-8F6EDDFBE4F2}    PSFactoryBuffer
  {242025BB-8546-48B6-B9B0-F4406C54ACFC}    InkSettings Class
  {24264891-E80B-4fd3-B7CE-4FF2FAE8931F}    PSFactoryBuffer
  {24400D16-5754-11d2-8218-00C04FB687DA}    Index Cleaner Prop Bag
  {2475A152-2C35-4489-BCBA-A269BD3F5BA4}
  {24954E9B-D39A-4168-A3B2-E5014C94492F}    OOBE Upgrade Password Page
  {24AC8F2B-4D4A-4C17-9607-6A4B14068F97}    CortanaExperienceFlow
  {24ad3ad4-a569-4530-98e1-ab02f9417aa8}
  {24CA8AEF-F6D8-4732-8DB5-9D83EFD8CFBC}    OOBE Eula Wizard Page
  {24D568C5-F3AE-4F91-9CD9-AA18876DA7C2}    HomeGroup Control Panel
  {24DC3975-09BF-4231-8655-3EE71F43837D}    Video Mixing Renderer 9 Device Segment
  {24DF3111-8474-4955-AA18-F6750BAD2A2B}    DsmAppInstallProgress Factory
  {250e91a0-0367-11cf-abc4-02608c9e7553}    WinNT Namespace Object
  {25150040-b8f1-418e-af61-b51071ac1ee2}    IEnumExplorerCommand Object On Menu
  {251b1498-5cba-4bee-8242-2f57773151aa}    CFolderInformationProxy
  {25256c24-3b75-49b3-a433-4bb2f8865896}    CLSID_StartMenuProvider
  {25336920-03F9-11cf-8FD0-00AA00686F13}    HTML Document
  {25336921-03F9-11CF-8FD0-00AA00686F13}    Microsoft HTML Document 6.0
  {25585dc7-4da0-438d-ad04-e42c8d2d64b9}    Client application shell extension
  {2559a1f0-21d7-11d4-bdaf-00c04f60b9f0}    Search
  {2559a1f2-21d7-11d4-bdaf-00c04f60b9f0}    Windows Security
  {2559a1f3-21d7-11d4-bdaf-00c04f60b9f0}    Run...
  {2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}    E-mail
  {2559a1f7-21d7-11d4-bdaf-00c04f60b9f0}    Set Program Access and Defaults
  {2559a1f8-21d7-11d4-bdaf-00c04f60b9f0}
  {255a6fda-6f93-4e8a-9611-ded1169eefb4}    MF Dolby AC-3 Sink Class Factory
  {25642426-028D-4474-977B-111BB114FE3E}    PSFactoryBuffer
  {2594513E-13AE-4700-B413-8D86A574BA98}    CLSID_MIMEUUEncoder
  {25983561-9D65-49CE-B335-40630D901227}    Microsoft IMAPI v2, Raw CD Image Creator
  {25ab468c-3974-4075-be50-193135461727}    Show/hide menu bar command invocation
  {25B25D91-69A2-47fa-A375-FDC98189A06F}
  {25BAAD81-3560-11D3-8471-00C04F79DBC0}    MediaDevMgr Class
  {25BE9228-00AF-11D2-BF87-00C04FD8D5B0}
  {25CBB996-92ED-457e-B28C-4774084BD562}    GenericProvider
  {25dead04-1eac-4911-9e3a-ad0a4ab560fd}    CLSID_TrayNotify
  {25E609E0-B259-11CF-BFC7-444553540000}    Microsoft DirectInput
  {25E609E1-B259-11CF-BFC7-444553540000}    Microsoft DirectInputDevice
  {25E609E4-B259-11CF-BFC7-444553540000}    Microsoft DirectInput8
  {25E609E5-B259-11CF-BFC7-444553540000}    Microsoft DirectInput8
```

Page 41

SOFTWARE OUTPUT.txt

```
{25EC352E-72E1-4724-9A28-4AE730072149}
{25ecf786-a925-4706-a269-eef5ad6899db}    ImeCommonAPIClassFactory
{25F51130-BE08-49a9-B37B-1C4A49FEBD5B}    Microsoft IME Japan SD Suggestion Data
Source
{25F843F3-1ED6-4B4E-8749-DF294C7FEB30}    SpStreamFormatConverter Class
{260eb9de-5cbe-4bff-a99a-3710af55bf1e}    InstallAgent
{2633B17B-846E-428C-8F60-7B8418F9AE89}    CLSID_MIMEBinHexEncoder
{263A4743-BC0D-40b6-8F7F-1B2135C204D2}    Search Option System Files Command
{26445657-50E1-4C9F-8378-FF028FD26816}    MTF Property Bag
{264FFAF3-9A9C-42B7-AEDB-34896CDBC7C1}    AppsFolder Verb Handler
{265011AE-5481-4f77-A295-ABB6FFE8D63E}    MS AMRNB Decoder MFT
{26671179-2ec2-42bf-93d3-64108589cad5}    ShellItemArray Shell Namespace helper
{266C72D4-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Log File Event Consumer
Provider
{266C72E5-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Command Line Event Consumer
Provider
{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM NT Event Log Event Consumer
Provider
{266C72E7-62E8-11D1-AD89-00C04FD8FDFF}    Microsoft WBEM Active Scripting Event
Consumer Provider
{267cf8a9-f4e3-41e6-95b1-af881be130ff}    Location Folder
{267DB0B3-55E3-4902-949B-DF8F5CEC0191}    Custom Composition Segment from WebDVD
Device Segment to Standard Video Renderer Device Segment
{26A1F020-DDD8-472D-8B7C-2F98B80024F3}    MF MPEG2 Parser Class Factory
{26bdc675-a557-411c-975f-80c4a63428f7}    PSFactoryBuffer
{26DFFE05-90B8-4744-8A17-50B9B64E0009}    SystemMonitor Class
{26EC0B63-AA90-458A-8DF4-5659F2C8A18A}    BDA Tuning Model Digital Cable Tune
Request
{26ED43EA-45C6-4EF6-9E9B-1740366C98BF}
{26EE0668-A00A-44D7-9371-BEB064C98683}    Control Panel
{26EEC7CE-6C67-4568-BA8F-52BEA143D756}    SpW3CGrammarCompiler Class
{26fdc864-be88-46e7-9235-032d8ea5162e}    Merged Folder
{27016870-8E02-11D1-924E-00C04FBBBFB3}    MS Remote
{270411D9-9832-48D5-BC1C-CE606B00F42E}    PSFactoryBuffer
{27171325-5F06-407C-AA8F-61154A674DE2}    PrintPlatformDocumentTargetFactory
{271C3902-6095-4c45-A22F-20091816EE9E}    MPEG4 Byte Stream Handler
{27354124-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Stream interleave
utility
{27354125-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Stream concatenation
utility
{27354126-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, PRNG based stream
{27354127-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Zero Stream
{27354128-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, RAW Disc-At-Once CD
Writer
{27354129-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Audio CD Writer
{2735412A-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Standard Data Writer
{2735412B-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Media Erase
{2735412C-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Write Engine
{2735412D-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, CD DVD Device Object
{2735412E-7F64-5B0F-8F00-5D77AFBE261E}    Microsoft IMAPI v2, Disc Master
{27354130-7F64-5B0F-8F00-5D77AFBE261E}    PSFactoryBuffer
{2737EE87-ABA3-4F28-89A6-C370484D85F9}    Compressed File Extract To verb handler
{273eb5e7-88b0-4843-bfef-e2c81d43aae5}    Application Startup Link
{2744BC6A-4039-11E3-ABAD-8CFB6188709B}    Collection Staging Manager
{274fae1f-3626-11d1-a3a4-00c04fb950dc}    ADs LDAP NameTranslate Object
{27569A8A-5891-4ad0-A0CE-74D6CBC035A9}    ToolTipOpenedEvent Class
{275AF033-1C37-48ED-91F7-8E23C5D9B382}    EmailClient
{275C23E2-3747-11D0-9FEA-00AA003F8646}    Multi Language Support
{2764BCE5-CC39-11D2-B639-00C04F79498E}    Generic Graph Composition Segment
{2769280B-5108-498c-9C7F-A51239B63147}    PSFactoryBuffer
{276C88CA-7533-4A86-B676-66B36080D484}
{276D4FD3-C41D-465F-8CA9-A82A7762DF32}    Cloud Change Wnf Monitor
{276FBFC1-D71F-4619-A7C1-0181077EE283}    Microsoft.Windows.Diagnosis.ManagedHost
```

Page 42

SOFTWARE OUTPUT.txt
```
{2781761E-28E0-4109-99FE-B9D127C57AFE}  Windows Defender IOfficeAntiVirus
implementation
{2781761E-28E2-4109-99FE-B9D127C57AFE}  Windows Defender IAmsiUacProvider
implementation
{27949969-876A-41D7-9447-568F6A35A4DC}
{2797B627-B7FA-4CBF-9472-6B8ACFDF3E41}  SpSharedRecoContext Class
{2797CF92-415A-43e6-A8F7-A5FAAB783719}  CPartitionPropPages Class
{27AAD1C8-3564-4A15-B0B8-F73F90FB95A7}  SpPhraseInfoBuilder Class
{27c98999-2895-4829-b080-5a8b65bd3db0}  AudioRateConvertCMPT Class
{27D62E77-6AFE-4AAE-AF27-E6CC20A884D9}  SpVAMaster Class
{27E097EC-6D59-4F02-8457-FC647BCB64FA}  DetectionHandler
{27E4B0FF-4E29-4998-A7A5-5979E8F8A630}  WiFi Notification Activator
{27F86E83-F66E-455B-BE1F-1ED899C48A2B}  CLSID_LockScreenAppPositioner
{27FE144C-9CAD-4EA6-8232-912FE8A96873}
{27FEB6AA-3BF1-4E2C-9E12-07EABEB0FBDB}  CLSID_ModalWindowExperienceOptions
{280A3020-86CF-11D1-ABE6-00A0C905F375}  AC3 Parser Filter
{280A7B65-8F00-438F-989B-8EAF9E438A71}
{280ECF1B-B8F6-41B6-BC14-0E58035C4DCC}  Package State Change Handler
{2854F705-3548-414C-A113-93E27C808C85}  Enhanced Storage Context Menu Handler
Class
{286AA738-2928-49af-A410-4118F5C31626}  Dot3 Helper Class
{286F484D-375E-4458-A272-B138E2F80A6A}  DirectPlay8Peer Object
{28803F59-3A75-4058-995F-4EE5503B023C}  Bluetooth Devices
{28890E39-A124-4216-B3D8-686F4203AD20}  NarratorPropertyChangeHandler Class
{288a2d5f-253c-46b4-b58c-2ced3180b993}  CMI IInstaller
{288B5845-2831-42c3-861B-0ADB30446513}  ValueChangeEvent Class
{289228DE-A31E-11D1-A19C-0000F875B132}  ListPad class
{28953661-0231-41DB-8986-21FF4388EE9B}  MSVidCtl Analog Capture to Encoder
Composition Segment
{289978AC-A101-4341-A817-21EBA7FD046D}  Sync Center Conflict Folder
{28AB0005-E845-4FFA-AA9B-F4665236141C}  Analog Audio Component Type
{28AF2E16-0190-44F4-9CED-08AF91145361}  RA Helper Class
{28BCCB9A-E66B-463C-82A4-09F320DE94D7}  F12 Developer Tools
{28BE6EDE-2FCA-4493-B462-CB5F7E680973}  CLSID_MIMEQuotedPrintableEncoder
{28D18BFA-85E3-4419-9AFD-7ECCE53F8D13}  SpMMAudioInLegacy Class
{2933BF91-7B36-11D2-B20E-00C04F983E60}  Free Threaded XML DOM Document
{2933BF94-7B36-11D2-B20E-00C04F983E60}  XSL Template
{293ccd4b-0d59-43c0-997e-3449c780ac65}  Authenticate Server UI class
{294935CE-F637-4E7C-A41B-AB255460B862}
{2959380c-1567-40ec-80b0-05907ad6f9de}  IP Neighbor Helper Class
{2965e715-eb66-4719-b53f-1672673bbefa}  Results Folder
{2968B3C3-CC07-40BE-B78F-094B7C310479}
{297EE78C-BA95-4E94-81D3-D6E7F089C7B5}  Reserved Priority Static Db Sync Task
{2984A9DB-5689-43AD-877D-14999A15DD46}  RecoExt Class
{299D0193-6DAA-11d2-B679-006097DF5BD4}  FTP IDataObject impl
{29B5828C-CAB9-11D2-B35C-00105A1F8177}  Microsoft WBEM (non)Standard Marshaling
for IWbemUnboundObjectSink
{29CE1D46-B481-4AA0-A08A-D3EBC8ACA402}  Shell User Enumeration Object
{29D365AE-D23B-4004-8658-5ED2A59CD77C}  RASGCW Change Password Class
{29EA1611-529B-4113-8EE3-EE0F6DD2C715}  NCProvider Class
{29F06F0C-FB7F-44A5-83CD-D41705D5C525}  PropGroupManagerObject Class
{2A005C11-A5DE-11CF-9E66-00AA00A3F464}  Windows.Devices.HumanInterfaceDevice
{2A038320-5727-4FDC-B703-1EC222C6911F}  Mpeg4s Decoder DMO
{2a11bae2-fe6e-4249-864b-9e9ed6e8dbc2}  CivicAddressReportFactory Class
{2A11F42C-3E81-4ad4-9CBE-45579D89671A}  XML Paper Specification Filter Persistent
{2A196062-812A-4249-B04A-797971DC466C}
Handler
{2A3EFC7B-7CEB-496A-9E69-DC40AD179F51}  CLSID_InstallAccountPictureExecute
{2A614240-A4C5-4C33-BD87-1BC709331639}  Bidi Spooler APIs
{2A6F3A80-5976-11D2-9524-0060081840BC}  Silence
{2A744BD8-158A-4bbf-9513-4A656F6C01D7}  Windows Desktop Search Scope Manager
{2A7B042D-578A-4366-9A3D-154C0498458E}
System.Management.Instrumentation.ManagedCommonProvider
```
Page 43

SOFTWARE OUTPUT.txt

```
{2aa2b5fe-b846-4d07-810c-b21ee45320e3}   Network Provisioning via XML Class
{2AABFCD0-1797-11D2-ABA2-00C04FB6C6FA}   WSecEdit Security Configuration Class
{2ACFC431-A2E7-4FC6-8C4B-0B4BD201A797}   First Logon Sync
{2AF141DE-8433-4FE1-A14B-D4AF981AB2F5}   OOBE ConnectedUser Plugin
{2af6bcaa-f526-4803-aeb8-5777ce386647}   EapMschapv2Cfg Class
{2AFCECBA-ABA5-404B-8F4F-15BECC9FEE20}   Microsoft NDIS IM Platform WMI Provider
{2B1C6F4F-4F0D-490F-8D88-A3EAF66130AC}
{2B1FFCE5-DD0F-4f1f-B150-A87AE69CE009}   Toggle Recycle confirmations
{2B20FE1A-1B2C-4DC5-8595-616B0E182FD1}   MSASR Locale Handler Class (1036)
{2b2cad40-19c1-4794-b32d-397e41d5e8a7}   User OOBE Controller
{2B32ECC3-C3BB-4701-82BB-EB7FE370D999}   Action Execution Broker
{2B4099B4-ABED-4014-881E-AB96D7CC4E48}   Registry Setting Monitor
{2B445657-7159-42A1-84F0-538E82EE5DE9}   MTF Composite
{2B489FDC-FBCE-4FB9-878B-D957619FD043}   InstallationHandler
{2B4F54B1-3D6D-11d0-8258-00C04FD5AE38}   Shell BindStatusCallback Proxy
{2B6DA137-316E-458B-A0AB-BE48C8EC39B9}   Display Control Panel
{2b8f8a9e-51b6-46db-9d45-ffb33e023823}   HDCP Manager
{2BB8B28A-58DC-449C-A89B-DAEFD0A8933D}
{2BC0EF29-E6BA-11d1-81DD-0000F87557DB}   Convolution
{2BD40F38-DE45-429D-9D04-24F7C24C78FD}   PSFactoryBuffer
{2BE1981C-CCF9-4D8B-8DA2-E217287AD983}   MTF Suggestion Context Property
{2be6c86f-1e02-40c2-9394-e98270c4d4e6}   MDEServer Factory
{2C256447-3F0D-4CBB-9D12-575BB20CDA0A}   FaultrepElevatedDataCollection
{2C3E140B-7A0D-42d1-B2AA-D343500A90CF}   CTrkEvntListener Class
{2C63E4EB-4CEA-41B8-919C-E947EA19A77C}   BDA Tuning Model MPEG2 Tune Request
Factory
{2C673043-FC2E-4d67-8920-517D24DEBD2C}
{2C731933-62A6-31A0-AFE1-1034F46361D2}
{2C786341-0E36-4BE8-AA51-524CC1F2AE15}   NowPlayingSessionManager Desktop Local
Provider
{2c86c843-77ae-4284-9722-27d65366543c}   Setting Profile Handler
{2C875213-FCE5-11d1-A0B0-00C04FA31A86}
{2c932742-413c-4b70-82c9-252094ed4c3c}   Install Office Scheduled Task Handler
{2C941FC5-975B-59BE-A960-9A2A262853A5}   FileSystemImage Class
{2C941FCE-975B-59BE-A960-9A2A262853A5}   BootOptions Class
{2C941FD4-975B-59BE-A960-9A2A262853A5}   PSFactoryBuffer
{2CA8CA52-3C3F-11D2-B73D-00C04FB6BD3D}   AudioInputMixer Property Page
{2cba6529-b64d-4c0e-8f48-043b845ef9b3}
Windows.Devices.Bluetooth.Background.GattCharacteristicNotificationTriggerDetails
{2CD19B3E-3897-4EAB-9AC6-B1438F520CA1}   CLSID_WindowsStoreUserApps
{2CD39202-3A2F-4935-9A86-65B919919A7F}   WebTokenRequestResult Object
{2CFD5F1D-BFAA-4B72-B035-6B691F3A204C}   PSFactoryBuffer
{2d05c0a1-f85f-4830-b3e0-dc26e701d9aa}   CExtensionHandler
{2D0F7985-9EE6-427C-AAAA-A9D72CBFA853}
Windows.Security.Credentials.UI.UserConsentVerifier PSFactory
{2D11CF10-4FE0-45B2-88DF-6FFBF92BE9AB}   WaitDialog
{2D12DD17-6C4E-456E-A953-D210E3C64176}   SpCommunicator Class
{2D1F634B-BA35-4BA0-A3B4-B03AC5FE724A}   DUN Device Center Context Menu Handler
{2D20F990-DA11-4B00-A082-C548EDC78428}   PSFactoryBuffer
{2D2E24CB-0CD5-458F-86EA-3E6FA22C8E64}   VMR Allocator Presenter 9
{2d3468c1-36a7-43b6-ac24-d3f02fd9607a}   A collection of IUnknown objects that can
be enumerated
{2D3F8A1B-6DCD-4ED5-BDBA-A096594B98EF}
{2D4156A2-897A-11DB-BA21-001185AD2B89}   Network List Manager Snapin
{2D4156A5-897A-11DB-BA21-001185AD2B89}   Network List Manager Snapin About
Interface
{2D533768-8BD9-4D3D-8754-25E0CF5A1290}   CloudExperienceHost Sign-In Identities
Default Implementation
{2D709E52-123F-49b5-9CBC-9AF5CDE28FB9}   Microsoft MPEG Video Decoder MFT
{2DA1964A-7232-48BF-9946-D0510557C492}   IHVNonUIFinishPage Class
{2DA6AA7F-8C88-4194-A558-0D36E7FD3E64}   Create and edit Wireless policies
{2DB47AE5-CF39-43C2-B4D6-0CD8D90946F4}   StreamBufferSink
{2DB5E62B-0D67-495F-8F9D-C2F0188647AC}
```

Page 44

SOFTWARE OUTPUT.txt

```
{2DD80115-AD1E-41F6-A219-A4F4B583D1F9}    PSFactoryBuffer
{2DDC6BB3-BFCF-4F30-8E9E-B78431C8CC4D}    PrintTaskConfigurationProxyServer
{2de55398-137e-4c4c-bf72-5cc7f18d9109}    Navigation Pane Expand to Current Folder
Explorer Command
{2DE92DB3-CD3E-4ad6-80F9-089036E1C81E}    CLSID_HomeGroupRoamedPassword
{2DEA658F-54C1-4227-AF9B-260AB5FC3543}    Microsoft PlaySoundService Class
{2df7b51e-797b-4d06-be71-d14a52cf8421}    MF Store Object Activate
{2dfb3a35-6071-11d1-8c13-00c04fd8d503}    Microsoft Locality Extension
{2E095DD0-AF56-47e4-A099-EAC038DECC24}    AnalogCable Class
{2E1271D5-2FF2-4EA4-9647-C67A82A2D85C}
{2e167ea7-85e3-4395-995a-77af9875d79a}
{2E17C0EF-2851-459b-A3C8-27A41D4BC9F7}    Windows Theme Manager API
{2e2294a9-50d7-4fe7-a09f-e6492e185884}    rtf persistent handler
{2E4D68DD-F8F7-4B7F-8BF9-E71B84A97F17}    ProxyStubFactory
{2e5e84e9-4049-4244-b728-2d24227157c7}    UPnPRemoteEndpointInfo
{2e7583c7-7eba-4a1a-8468-d03d28477e6f}    Shell settings migration
{2E7700B7-27C4-437F-9FBF-1E8BE2817566}    RandomBars
{2E8EA1E5-F406-46F5-AF10-661FD6539F28}    WSecEdit Local Security Settings Class
{2E8FCB18-A0EE-41AD-8EF8-77FB3A370CA5}    CLSID_ShellExperienceManagerFactory
{2E9E59C0-B437-4981-A647-9C34B9B90891}    Sync Setup Folder
{2EAF57E6-3E96-4D68-8F06-ADC55A842EF9}    ChsPinyinDS
{2EBDEE67-3505-43f8-9946-EA44ABC8E5B0}    PSFactoryBuffer
{2ED326ED-C4C0-434a-B4CE-FB0318D725A7}    PSFactoryBuffer
{2eeb4adf-4578-4d10-bca7-bb955f56320a}    WMAudio Decoder DMO
{2EEEED04-0908-4cdb-AF8F-AC5B768A34C9}    Drm Scheme Handler
{2F0888F4-2C5B-4353-A395-40CF3B6BA29E}    CLSID_PropertyStoreXml
{2F096B28-C65D-4C05-A37E-7E88735E32FA}    Clear Recent Documents Command
{2F2165FF-2C2D-4612-87B2-CC8E5002EF4C}    Advanced Indexing Options Dialog Object
{2F29854D-D87F-4B47-8BF8-0C25AEB83FB0}    CloudExperienceHost Sign-In Identities
Implementation
{2f2dc38b-34d2-462c-add4-f74cc15510a1}    SuggestPopup
{2F5C3DEB-80B1-484A-9843-BBCDF6CAA0B2}    AEP Setting Handler
{2F5E64E3-0B46-4DAF-AEA6-721994E5AC8B}    RootCATrustedCertificates
{2F63C206-752B-4B26-9DA7-CD264895A7C8}    RASGCW Progress Class
{2F6CE85C-F9EE-43CA-90C7-8A9BD53A2467}    FileHistoryDataSource
{2f712f0f-ed71-474b-9529-9b9627ed0a6b}    System Setting Sync Handler
{2F7ED5E3-06C9-4B61-97DB-067CC8AE0664}    OOBE End Plugin
{2F86B8BD-EFF5-4C07-8FA5-60788517EF95}    Microsoft Print Management WMIv2 Provider
{2f8891f3-f692-450e-a222-ff28d9daaaf8}    Location Picker Class
{2f893820-7089-46cc-a6e8-c4aae45f151b}    DTC MMC Snap-in
{2F93C02D-77F9-46B4-95FB-8CBB81EEB62C}    DevicesFlow
{2F94D7B0-BF63-11D1-A6A2-00C04FB9988E}    EndpointsTable Class
{2FAE8AFE-04A3-423a-A814-85DB454712B0}    MS AMRNB Encoder MFT
{2FB21955-33A2-46A0-8F60-B475DC33FD5A}    PSFactoryBuffer
{2FFD1C83-BC94-4E39-AEE7-BE162E7D1F84}    SpWASAudioLoop Class
{300a81e6-a674-4d84-9eed-0337389e7e66}    Desktop Application Activator
{301056D0-6DFF-11D2-9EEB-006008039E37}    MJPEG Decompressor
{301B94BA-5D25-4A12-BFFE-3B6E7A616585}    Microsoft RDP Client Control
(redistributable) - version 10
{301F77B0-A470-11D0-8821-00A0C903B83C}    Encode Date Array Class
{30276b4f-f25c-457c-a4b7-08574f8ea528}    CLSID_ResultSetFactory
{3028902F-6374-48b2-8DC6-9725E775B926}    IE AutoComplete
{3037B4CD-A40B-401B-B676-2017EE8FAFF4}    Wordpad DOCX Filter
{304FC8AB-6643-4DAA-9027-4B21389DCB2D}    IRemoveDeviceElevatedHandler_PSFactory
{3050F391-98B5-11CF-BB82-00AA00BDCE0B}    Microsoft HTML Window Security Proxy
{3050F3B2-98B5-11CF-BB82-00AA00BDCE0B}    Microsoft HTML Javascript Pluggable
Protocol
{3050f3B3-98b5-11cf-bb82-00aa00bdce0b}    %Microsoft Image Element Browse Property
Page%
{3050f3B4-98b5-11cf-bb82-00aa00bdce0b}    %Microsoft Document Browse Property Page%
{3050f3BB-98b5-11cf-bb82-00aa00bdce0b}    %Microsoft Anchor Element Browse Property
Page%
{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B}    Microsoft HTML Resource Pluggable Protocol
```

Page 45

SOFTWARE OUTPUT.txt

```
{3050F3C2-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML DwnBindInfo
{3050F3D6-98B5-11CF-BB82-00AA00BDCE0B}  IImgCtx
{3050F3D9-98B5-11CF-BB82-00AA00BDCE0B}  MHTML Document
{3050f3DA-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML Mailto Pluggable Protocol
{3050F406-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML About Pluggable Protocol
{3050f499-98b5-11cf-bb82-00aa00bdce0b}  Microsoft HTML Recalc
{3050F4CF-98B5-11CF-BB82-00AA00BDCE0B}  PeerFactory Class
{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B}  HTML Application
{3050f4e1-98b5-11cf-bb82-00aa00bdce0b}  HtmlDlgHelper Class
{3050f4f5-98B5-11CF-BB82-00AA00BDCE0B}  Trident HTMLEditor
{3050f4f8-98b5-11cf-bb82-00aa00bdce0b}  Microsoft Html Component
{3050f5be-98b5-11cf-bb82-00aa00bdce0b}  DownloadBehavior Class
{3050F5C8-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTA Document 6.0
{3050f664-98b5-11cf-bb82-00aa00bdce0b}  LayoutRect Class
{3050f667-98b5-11cf-bb82-00aa00bdce0b}  Microsoft Html Popup Window
{3050f67D-98b5-11cf-bb82-00aa00bdce0b}  Microsoft Html Document for Popup Window
{3050f6b3-98b5-11cf-bb82-00aa00bdce0b}  Template Printer class
{3050f6cd-98b5-11cf-bb82-00aa00bdce0b}  HeaderFooter class
{3050f6d4-98b5-11cf-bb82-00aa00bdce0b}  DeviceRect Class
{3050f819-98b5-11cf-bb82-00aa00bdce0b}  HtmlDlgSafeHelper Class
{30510483-98B5-11CF-BB82-00AA00BDCE0B}  Microsoft HTML Element Context Stream
{30562646-f7b5-4a62-8ced-6f30a70587c5}  CImeDictionaryFileCopier Class
{30590066-98b5-11cf-bb82-00aa00bdce0b}  SVG Document
{30590067-98b5-11cf-bb82-00aa00bdce0b}  XHTML Document
{3059ACB9-9875-44CC-ABA9-EAA6EFBEBA39}
{30655864-f8cd-45f9-b7d6-6721acb69c5e}  Network Connection Helper Class
{30766BD2-EA1C-4F28-BF27-0B44E2F68DB7}  Windows Search Root
{3080F90D-D7AD-11D9-BD98-0000947B0257}  Show Desktop
{3080F90E-D7AD-11D9-BD98-0000947B0257}  Window Switcher
{30B33640-5250-4328-92C5-A1618E406A3A}  SystemAlertEvent Class
{30C3B080-30FB-11d0-B724-00AA006C1A01}  CoMapMIMEToCLSID Class
{30d49246-d217-465f-b00b-ac9ddd652eb7}  Identity Store
{31143611-AC65-4568-AE76-8A9DAD50EA88}  CLSID_NotificationController
{31220067-EE3A-4ED7-B579-103D74930CB5}  HomeGroup Task
{3124C396-FB13-4836-A6AD-1317F1713688}  SAX XML Reader 3.0
{312A6884-4ABE-4C4E-AE73-C69874C8318B}  Staging Setting Handler
{31337EC7-5767-11CF-BEAB-00AA006C3606}  AuthHost
{31350404-77AC-4471-B33A-9020A2EDA1D1}  MSASR Locale Handler Class (3082)
{3140F5B6-093F-4F94-9141-5DF9EE10BC27}  MSASR Locale Handler Class (1033)
{31430c59-bed1-11D1-8De8-00C04FC2E0C7}
{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}
{317F3AA1-A5F5-4310-9401-BAE5DAC386C6}  text persistent handler for mapi email
{3185a766-b338-11e4-a71e-12e3f512a338}  Flight Settings API Broker
{31879719-E751-4DF8-981D-68DFF67704ED}
{31b11d80-9ed7-44f7-b1cd-c95992a738b9}  Layer Composer
{31b231f6-546d-4f9b-ac95-0f963d72559c}  Sync Command State Handler
{320690f4-8d7b-4f55-a98d-89ebb01fa776}  CStorageStreamTransactionProxy
{323CA680-C24D-4099-B94D-446DD2D7249E}  Favorites
{3240F7D1-E591-4807-8370-08625D21CAAB}  Windows.Energy.ProxyStubFactory
{32433977-2283-4853-8a6d-e7f4cc3053bc}  FhRehydrationTaskHandler Class
{325524D7-854E-4989-9219-E1E1B8501823}  PSFactoryBuffer
{32557D3B-69DC-4F95-836E-F5972B2F6159}
{3261BF13-9B3E-4DD5-B6D3-0006F3FFE8BC}  OOBE Auth Proxy Wizard Page
{32624F4B-F1D5-4877-989E-555640109D2B}  Windows Photo Viewer Gallery Interface
{32665929-D77E-4ab5-8C08-FBF409B8A233}
{3279762A-C6C8-4274-A2FB-FD390DAEB7E7}  CLSID_ModalWindowExperienceManager
{3283EEBF-E67D-31AC-8481-A968F3A77E9A}
{328489c8-f25e-44b5-93d4-8f811b4dc326}  Battery Status Provider
{328B0346-7EAF-4BBE-A479-7CB88A095F5B}  LayoutFolder
{329B80EC-2230-47B8-905D-A2DCF5171C6F}  CLSID_ImmersiveSplashScreen
{32A8DF4D-2E8C-4983-A156-912D7FAB10EA}  Connection Class
{32B0C344-A3BB-4F6E-B8D9-E883BC150EEA}  OOBE ConnectedUser Wizard Page
{32B533BB-EDAE-11d0-BD5A-00AA00B92AF1}  AP Class Install Handler filter
```

Page 46

```
                         SOFTWARE OUTPUT.txt
    {32BA16FD-77D9-4AFB-9C9F-703E92AD4BFF}   CtTuner Class
    {32BAED44-34B5-11D3-9315-00C04F72D6CF}   MSSCP Class
    {32be5ed2-5c86-480f-a914-0ff8885a1b3f}   RDPViewer Class
    {32BF9005-7CC6-4F1D-A71D-2D912252B7BE}   Notification Center UI
    {32C5A81F-27C0-4E66-A894-786F646F1236}   PSFactoryBuffer
    {32d186a7-218f-4c75-8876-dd77273a8999}   Microsoft AAC Audio Decoder MFT
    {32DA2B15-CFED-11D1-B747-00C04FC2B085}   Script Encoder Object
    {32E7DC13-1E22-4D7E-8AC7-D2E718DE8042}   InfraProfileExistsErrorPage
    {32EAC0F0-1C2B-4775-942E-0AC11121A0F4}   Token Broker Monitor
    {3318360C-1AFC-4D09-A86B-9F9CB6DCEB9C}   ClassicLangBar
    {331E8B29-D4C3-4278-B005-671BB919C320}   Default Printer Provider
    {331E9F3D-9351-4A4D-A2CA-75A16BAFF7BB}
    {332A1615-9FCB-4D57-BD09-EA10759BC2B6}   HighlightCursorInproc Class
    {3336B8BF-45AF-429f-85CB-8C435FBF21E4}   ClassicW Class
    {333C7BC4-460F-11D0-BC04-0080C7055A83}   Tabular Data Control
    {333E6924-4353-4934-A7BE-5FB5BDDDB2D6}
    {334125C0-77E5-11D3-B653-00C04F79498E}   BDA Data Services Feature Segment
    {334796A6-31DC-4B5D-8FD7-14E82186417C}   MTF Dynamic Dictionary Data Source for
Contacts
    {334857cc-f934-11d2-ba96-00c04fb6d0d1}   ADs DN With String Object
    {334AC349-574E-4CD6-B6EB-C7EDD7BDA93F}
    {336475D0-942A-11CE-A870-00AA002FEAB5}   MPEG-I Stream Splitter
    {337448ee-2a70-43f7-99f9-40f2857950b9}   JScript Language
    {33831ED4-42B8-11D2-93AD-00805F853771}   Microsoft NT DS Class Associations
Provider for WBEM
    {338B40F9-9D68-4B53-A793-6B9AA0C5F63B}   Delivery Optimization Mgmt Class
    {33ADC7D5-BAF1-4661-9822-1FD23E63B39F}   Language Components Installer Com Handler
    {33BCC8EC-0D01-4E10-AD3D-4DAF749873ED}   Browser Application State
    {33C4643C-7811-46FA-A89A-768597BD7223}   PSFactoryBuffer
    {33C53A50-F456-4884-B049-85FD643ECFED}   TF_InputProcessorProfiles
    {33c86cd6-705f-4ba1-9adb-67070b837775}   Onex PLAP Smartcard Credential Provider
    {33de48c4-943f-4b96-8cd8-b117c94576cf}
    {33F3C8F8-27A1-4DF3-A525-E89CB18881A5}   Workspace Setup Discovery Page
    {33FACFE0-A9BE-11D0-A520-00A0D10129C0}   SAMI (CC) Reader
    {33fd0563-d81a-4393-83cc-0195b1da2f91}   UPnPDescriptionDocumentEx Class
    {341301BA-111C-408D-A8E3-14D1DDC62A6F}
    {3449A1C8-C56C-11D0-AD72-00C04FC29863}   MSDataShape
    {34568a1f-8d5a-4080-99c7-464e2cb40008}   PSFactoryBuffer
    {347CBD95-DD80-4144-81AF-AE803E633A00}   PSFactoryBuffer
    {3480A401-BDE9-4407-BC02-798A866AC051}   ShellServiceHostBrokerProvider
    {348ef17d-6c81-4982-92b4-ee188a43867a}   PrintDocumentPackageTargetFactory
    {34996c91-9897-40eb-944b-28b5c9308383}   Device Property Manager Class
    {34a3d570-67d9-4265-a9ee-8c3fa3dfeccf}   TravelLog
    {34AB8E82-C27E-11D1-A6C0-00C04FB94F17}
    {34c10250-4e26-4950-924d-c2d3651ca94f}
Windows.Networking.Sockets.ControlChannelTriggerResetEventDetails
    {34DEA897-7365-4f60-BA26-53DA4B89226D}   HardwareCapability
    {34e5efee-eb08-4714-878a-11bbcbfc592b}   CImeCommentServerPlugInLocal Class
    {34e6abfe-e9f4-4ddf-895a-7350e198f26e}   Microsoft Feeds Arbiter LoRi Broker
    {34E72398-AB74-43DA-8355-7F60D1BE3F73}
Windows.Networking.Connectivity.ProxyStubFactory
    {34F85D56-33E9-4CD0-BB19-D8C3BAA04025}   Developer License Launcher Proxy
    {3508C064-B94E-420b-A821-20C8096FAADC}   AtscPsipParser Class
    {35117bca-71f9-4399-8709-f380c7aaa8bd}   Screen Fade
    {3523c2fb-4031-44e4-9a3b-f1e94986ee7f}   Microsoft RDP Client Control - version 3
    {352EC2B7-8B9A-11D1-B8AE-006008059382}   Shell Application Manager
    {3540D440-5B1D-49cb-821A-E84B8CF065A7}   MSVidCtl Analog Capture to XDS Composition
Segment
    {354F7156-A4F6-47F5-A028-FE2000E92132}   PSFactoryBuffer
    {355DFFAA-3B9F-435c-B428-5D44290BC5F2}   WpcSettingsProvider Class
    {356F2F88-05A6-4728-B9A4-1BFBCE04D838}
    {35786D3C-B075-49b9-88DD-029876E11C01}   Portable Devices
    {35A069A1-A029-46AF-B531-454C0F66D61F}   Network Status Interface
                          Page 47
```

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {35b1d3bb-2d4e-4a7c-9af0-f2f677af7c30} | WNet Provider Class |
| {35B3DA31-0DB4-4420-AAB4-998A8571E059} | Start Layout Setting Handler |
| {35B78F79-B973-48C8-A045-CAEC732A35D5} | WDM HiPerf Provider |
| {35C61CC2-5851-4F2D-89B6-4F9BB4B4193F} | Microsoft Search Property System Change Notify Handler |
| {35cc8486-4fb1-11d3-a5da-00c04f88249b} | Microsoft Korean IME HandWriting Applet |
| {35CEC8A3-2BE6-11D2-8773-92E220524153} | |
| {361290c0-cb1b-49ae-9f3e-ba1cbe5dab35} | InfectionState WMI Provider |
| {3613F1D2-C9A5-4f41-A070-E5BB823B2E5B} | Deep Search Command |
| {361778EC-D741-4CE1-90F9-743435F56E13} | Remove Device Menu |
| {3631271D-DDD3-40f2-AC17-B13A3742BA62} | SmsDeviceRevocation Class |
| {366D4750-AB08-4957-BF80-82133AF2BC86} | NarratorTextPatternElement Class |
| {368D4A96-945D-4D76-A3F8-B29636EB9758} | Notification Platform Shell Component |
| {3692CA39-E082-4350-9E1F-3704CB083CD5} | |
| {369647e0-17b0-11ce-9950-00aa004bbb1f} | Neutral Word Breaker |
| {3697790B-223B-484E-9925-C4869218F17A} | |
| {36a479ef-8b67-4d01-8dda-753cfcb2dd96} | CLSID_FilteredItemFactory |
| {36BAA497-8C84-4700-96A1-88E1876EC5B9} | ProtocolActivatedEventArgs |
| {36CB6E0C-78C1-42B2-9943-846262F31786} | A-law ACM Wrapper MFT |
| {36f0bd14-d84d-468c-b79c-9990f3fa897f} | Multi Object Elevation Factory |
| {36F54939-CD3B-4C73-92D5-F9A389ED631C} | Enhanced Storage Autoplay Handler Class |
| {36F99745-23C9-4C9C-8DD5-CC31CE964390} | MF WAVE Sink Class Factory |
| {370A1D5D-DDEB-418C-81CD-189E0D4FA443} | VBI Codec. |
| {370BF38C-0451-42e8-9B03-0CAFA95081B6} | Sync root error resolution verb |
| {371CCB71-D045-45C5-9952-BB07B1711B0B} | PSFactoryBuffer |
| {3722c3b1-82e8-4022-8b27-1f8a68b44ac7} | CLSID_ProviderConfig |
| {372FCE38-4324-11D0-8810-00A0C903B83C} | CertConfig Class |
| {3730BBF8-631A-48FB-9085-E2143C11563B} | HomeGroup Task |
| {3734FF83-6764-44B7-A1B9-55F56183CDB0} | Sync Center (Internal) |
| {373984C9-B845-449B-91E7-45AC83036ADE} | XML Schema Cache |
| {374CEDE0-873A-4C4F-BC86-BCC8CF5116A3} | IE HomePageSetting |
| {374DE290-123F-4565-9164-39C4925E467B} | |
| {374EE8E8-DEA6-4DB7-B14A-B43EE3E8948E} | Process Lifetime Manager |
| {3756e7f5-e514-4776-a32b-eb24bc1efe7a} | State of built-in commands |
| {375ff002-dd27-11d9-8f9c-0002b3988e81} | WCN-Config Function Discovery Provider Class |
| {376666C8-61CF-4152-8398-7015FFE165EE} | NarratorCustom Class |
| {37708080-3519-4ED6-91D5-A64B643863FB} | Windows.Help.Runtime.CatalogRead |
| {37734C4D-FFA8-4139-9AAC-60FBE55BF3DF} | BlbEngine Class |
| {378E0446-5384-43B7-8877-E7DBDD883446} | Bundle Package API Factory Object |
| {37903486-85EE-4733-AEFC-8C4496F19DE4} | Windows.Web.ProxyStubFactory |
| {379E501F-B231-11D1-ADC1-00805FC752D8} | MsxmlIsland |
| {37A61C8B-7F8E-4d08-B12B-248D73E9AB4F} | Secure Http Scheme Handler |
| {37B0353C-A4C8-11D2-B634-00C04F79498E} | File Playback Device Segment |
| {37B03543-A4C8-11D2-B634-00C04F79498E} | Standard Video Renderer Device Segment |
| {37B03544-A4C8-11D2-B634-00C04F79498E} | Standard Audio Renderer Device Segment |
| {37de7045-5056-456f-8409-c871e0f8b0e0} | Trun Gateway Protocol Class |
| {37E92A92-D9AA-11D2-BF84-8EF2B1555AED} | Audio Renderer Advanced Properties |
| {37ea3a21-7493-4208-a011-7f9ea79ce9f5} | Open Containing Folder Menu |
| {38018C19-B0ED-489F-A9DC-96EBF886450B} | Modern IME CHS Setting Handler |
| {3807BD87-D141-439A-B711-25A053A020F7} | Language Setting Monitor |
| {38086A84-31E7-4C8E-BB0E-9758D634C7E1} | Notification Center Status |
| {38142214-ED63-4965-9214-1BBC06E130E9} | CLSID_BackgroundAccessManager |
| {381DDA3C-9CE9-4834-A23E-1F98F8FC52BE} | |
| {3829dfb4-9eed-434e-88c7-dcbe810b1a6e} | Control-Mousewheel Handler |
| {382AC1B5-9C16-4CCD-9D00-D5053977B8D6} | Microsoft MM Agent WMIv2 Provider |
| {384742B1-2A77-4CB3-8CF8-1136F5E17E59} | CLSID_HideInputPaneAnimationCoordinator |
| {384ea5ae-ade1-4e8a-8a9b-7bea78fff1e9} | CLSID_BinaryAutoList |
| {3852C2E2-4A16-4b11-8E71-F8904C37EC3D} | Copy-To Menu |
| {385906fb-1482-4f64-8a23-5d74e1ce1815} | Add Columns Explorer Command |
| {385A91BC-1E8A-4e4a-A7A6-F4FC1E6CA1BD} | DXTFilter |
| {38795471-5D0E-452d-BEF8-5339CAF9E30B} | NarratorComboBox Class |
| {3882134d-14cf-4220-9cb4-435f86d83f60} | Provides IPortableDeviceValuesCollection |

Page 48

SOFTWARE OUTPUT.txt

helper methods for portable devices applications and drivers
```
{388D606F-AF7B-4AD2-AC22-6B4FE70CE286}    Create and edit Wired policies
{389EA17B-5078-4CDE-B6EF-25C15175C751}
{38A98528-6CBF-4CA9-8DC0-B1E1D10F7B1B}
{38be0989-9830-49a8-985b-7741219fd0fb}    CMVKey
{38BFA80B-F989-45B2-AAFD-1E0C04E50E56}    Post Apps First Logon Sync
{38F03426-E83B-4E68-B65B-DCAE73304838}    Custom Composition Segment from Data
```
Services to Time Shift Sink
```
{38FE8128-B282-4A98-B2B0-0BAFB49815FD}    DsmUserTask Factory
{3901CC3F-84B5-4FA4-BA35-AA8172B8A09B}    DirectSound 8.0 Object
{39124E35-C31A-4D85-BF08-667CC504D997}
{3918D75F-0ACB-41F2-B733-92AA15BCECF6}    SpObjectTokenEnum Class
{39472C07-79C6-4924-96E6-41F699CBAD9C}    CLSID_ShellTargetingTracker
{394C052E-B830-11D0-9A86-00C04FD8DBF7}
{3957a5ba-4448-bec4-24ac-16c4f5784ef5}    CLSID_OOBECortanaManagerCOM
{397a2e5f-348c-482d-b9a3-57d383b483cd}    Hyper-V Application Health Monitor
{39981129-C287-11D0-8D8C-00C04FD6202B}    CLSID_CMAPIAcctImport
{39AE2AEA-D4D5-4DA0-AE47-C020E1BE4BE5}    CLSID_JetDatabaseSession
{39AEDC00-6B60-46DB-8D31-3642BE0E4373}    TsfServices
{39F8D76B-0928-11D1-97DF-00C04FB9618A}    Microsoft DTC Transaction
{3A04D93B-1EDD-4f3f-A375-A03EC19572C4}    MaskFilter
{3A30A0BD-0155-43A3-A9D6-E8434AEABA09}    LockScreen Media Transport Control
```
Notification Status Provider
```
{3a40a10e-ab54-4d64-a2a8-ec81ac256c22}
{3A410F21-553F-11d1-8E5E-00A0C92C9D5D}    IDMRemoteServer_PSFactory
{3A445657-23E2-4E1E-82AB-D1836874C536}    MTF Primitive
{3a59a18b-f03c-48cb-8aa7-181d35291fd7}    IIMECheckDefaultInputProfile
{3A5B4772-7946-4E58-9310-B0D423749C1D}    Microsoft.WINDOWS.SQLLITE.OLEDB.4.0
{3A614B00-FB18-46F3-950E-682A46A48B9F}    PSFactoryBuffer
{3a64898b-20a7-4384-894b-7273c3539f2f}    MIME Filter PersistentHandler
{3A66787A-8B15-4321-A09D-6E862D2DD2D4}    Projection Manager
{3A8CCCBC-0EFD-43a3-B838-F38A552BA237}    CTocEntryList
{3A9428A7-31A4-45E9-9EFB-E055BF7BB3DB}    BDA Tuning Model Channel ID Tune Request
{3ABEAFC4-F48F-4517-A9B0-8AD6A94A99A1}    Publication Services Data
{3AC83423-3112-4AA6-9B5B-1FEB23D0C5F9}    Default browser Sync Settings
{3ad05575-8857-4850-9277-11b85bdb8e09}    Copy/Move/Rename/Delete/Link Object
{3ADCE5CC-13C8-4573-B328-ED438EB694F9}    CAviTocParser
{3ADD1653-EB32-4cb0-BBD7-DFA0ABB5ACCA}
{3AE86B20-7BE8-11D1-ABE6-00A0C905F375}    MPEG-2 Splitter
{3B0FB8F1-8882-4C9D-9E35-6C23FB9D8110}    BDA Proxy UPnP 1.0 Event-base Streaming
```
Plugin
```
{3B1599F9-E00A-4BBF-AD3E-B3F99FA87779}    State of verb commands implemented by
```
IContextMenu
```
{3b176793-1c28-467d-bf13-ff0ac689e18b}    EAPSIM Identity UI class
{3B17FD9C-F7CF-4736-AF6B-616C2D1ED854}    Activation Broker Manager
{3B1B5147-715E-49e0-AE9F-ADF86724BB89}    CLSID_DateTimeIntervalGenerator
{3B2B6775-70B6-45AF-8DEA-A209C69559F3}    DirectPlay8LobbyClient Object
{3B2B92B7-5787-4eb5-931D-9F69E47497A9}    NarratorDockPattern Class
{3B4BE995-61E3-430C-8977-0B21E4427BE7}    PSFactoryBuffer
{3b517f36-1fd1-41a8-afb3-8b016072f218}    MiracastReceiver
{3B64E510-8192-4224-A7AD-67E9A86EC479}    Initialize Set Network Location Foreground
```
Control
```
{3B873591-9427-4418-A086-79175735738F}    SMB CIM provider
{3BAF3FB2-421B-42ca-86BF-EBC2BB2145D3}    FocusEventFilter Class
{3bb4118f-ddfd-4d30-a348-9fb5d6bf1afe}    Time Categorizer
{3BB46AD9-4D42-4EC6-B96B-68973FCD26F1}    RASGCW Failure Class
{3BBE95A4-C53F-11d1-B3A2-00A0C9083365}    TRUN Tx Begin Class
{3BBE95DA-C53F-11d1-B3A2-00A0C9083365}    Trun Gateway Tx Class
{3BBE95F5-C53F-11d1-B3A2-00A0C9083365}    Trun Gateway Tx Crash Recovery Class
{3BBE95FB-C53F-11d1-B3A2-00A0C9083365}    Trun Gateway Instance Class
{3BBE95FE-C53F-11d1-B3A2-00A0C9083365}    Trun Gateway Instance Scan Class
{3BC4EE9F-1FC1-44DB-81FA-AD94DEC7AF30}    CLSID_AppRep
{3BEE4890-4FE9-4A37-8C1E-5E7E12791C1F}    SpSharedRecognizer Class
```
Page 49

```
                        SOFTWARE OUTPUT.txt
{3BF043EF-A974-49B3-8322-B853CF1E5EC5}  Microsoft VolumeControlService Class
{3BF2A5F1-C95E-4F7B-B939-582DB5F32B81}
{3BFADDE5-09ED-42AE-8190-2E68B650CFE6}  CLSID_CortanaMapiHelper
{3bfe6eb7-281d-4333-999e-e949e3621de7}  Cert Password UI class
{3c2654c6-7372-4f6b-b310-55d6128f49d2}  Alphabetical Categorizer
{3C296D07-90AE-4FAC-86F9-65EAA8B82D22}  CSppExtComObj Class
{3C305196-50DB-11D3-9CFE-00C04FD930C5}  DirectDraw7 Object
{3C374A40-BAE4-11CF-BF7D-00AA006946EE}  Microsoft Url History Service
{3C3A70A7-A468-49B9-8ADA-28E11FCCAD5D}  RASrv Class
{3C4059B0-FB29-4EBA-9947-289E0D824E64}  Settings Flow
{3C4512DC-AEFA-4a1e-95CF-EDF896092447}  Recycle command
{3C4708DC-B181-46A8-8DA8-4AB0371758CD}  MSVidCtl SBE Source to Video Mixing
Renderer Composition Segment
{3c5edebe-16c6-4ee4-906b-436aa1f6ef9e}
{3C5F432A-EF40-4669-9974-9671D4FC2E12}  MMC Plugable Internet Protocol
{3c6859ce-230b-48a4-be6c-932c0c202048}  Sxs Store Class
{3C852D74-7E49-4FF3-BF21-81EF888078D4}  MPEval
{3CB169B3-17D9-4E47-8B93-2878998F69A2}  WebBrowserHandler Proxy
{3ccdfa5a-33ef-46d4-89c6-06298e2e539a}  AppServiceTriggerDetailFactory
{3CCF8A41-5C85-11d0-9796-00AA00B90ADF}  Shell DeskBarApp
{3CE74DE4-53D3-4D74-8B83-431B3828BA53}  TF_DisplayAttributeMgr
{3D07A539-35CA-447C-9B05-8D85CE924F9E}  Closed Captions Analysis Filter
{3D0C78BF-98BF-4B97-835E-E4269F8E038D}  PSFactoryBuffer
{3D0DB8B7-7484-42BE-BF61-3427A2459A2B}  BackgroundAccessManagerService
{3D112E22-62B2-11D1-9FEF-00600832DB4A}  MMCTask class
{3d154a2d-d911-437e-a30c-5f56a9b7081d}  Extract Const Icon Handler
{3D4C34BE-7208-4F3B-B74F-37AD231350EF}  CLSID_ClickNote
{3D813DFE-6C91-4A4E-8F41-04346A841D9C}  MXXMLWriter 3.0
{3D85CB81-C520-436f-8C9A-8292041A9BDD}  NarratorSimpleEdit Class
{3dad6c5d-2167-4cae-9914-f99e41c12cfa}  Include In Library Sub Context Menu
{3DBEE9A1-C471-4B95-BBCA-F39310064458}
{3DBFEF35-6F15-4453-BC19-D7AD5CC04756}  Connected Search Shell Service
{3DC09436-7D83-4BA0-ADDC-CD47F996C5BA}  AudioMeter Class
{3DC7A020-0ACD-11CF-A9BB-00AA004AE837}  The Internet
{3dd53d40-7b8b-11D0-b013-00aa0059ce02}  CDL: Asychronous Pluggable Protocol
Handler
{3dd6bec0-8193-4ffe-ae25-e08e39ea4063}  NPProvider
{3DD82D10-E6F1-11D2-B139-00105A1F77A1}  WMI instrumentation:
Win32_PowerManagementEvent
{3DECD5DD-A27B-48DC-8BAA-2682CFA265FF}  Workspace Setup Message Page
{3df11260-58db-46ca-85ee-35459e115b9c}  EAPHost Interactive UI class
{3dfdf296-dbec-4fb4-81d1-6a3438bcf4de}
{3E000D72-A845-4CD9-BD83-80C07C3B881F}  CMLUAUTIL
{3e0f30a5-6c0c-4daf-b41e-7b1011ed7e1c}  PnpObjectUpdateServer
{3E298C47-0DA7-4418-AAC7-7A6D1F800A14}
{3E458037-0CA6-41aa-A594-2AA6C02D709B}  SBE2FileScan
{3E4D4F1C-2AEE-11D1-9D3D-00C04FC30DF6}  oleprn Class
{3E54D3BF-8EFA-400f-B875-B86A309E1CBF}  NarratorSplitButton Class
{3E58004E-4CE5-4681-BA56-785A67F9F0DC}  playtomanager
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}  CMSTPLUA
{3E6147C9-902B-48BA-B1B8-5B1FFD874FB2}  Touchpad Gesture Provider
{3E669F1D-9C23-11d1-9053-00C04FD9189D}  DXSurface Modifier
{3e71f26d-136f-4545-813f-35276024b705}  XML Feed Subscribe Dialog
{3E784A01-F3AE-4DC0-9354-9526B9370EBA}  SAXAttributes 3.0
{3e83c6bd-8ef0-491c-b4a8-8853e9973829}  PSFactoryBuffer
{3EA48300-8CF6-101B-84FB-666CCB9BCD32}  OLE Docfile Property Page
{3EC569DC-6FB5-45D1-8B46-E122D27962E9}  CLSID_UAPSplashScreenEvents
{3EE60F5C-9BAD-4CD8-8E21-AD2D001D06EB}  InkObject Class
{3EE8CE0F-2507-42DE-A453-8F4D554256E8}  Default Device Manager
{3eef301f-b596-4c0b-bd92-013beafce793}  Desktop Undo Manager
{3EF76D68-8661-4843-8B8F-C37163D8C9CE}  Custom Composition Segment from CCA to
Stream Buffer Source
{3F30C968-480A-4C6C-862D-EFC0897BB84B}  Photo Extract Image
                          Page 50
```

```
                        SOFTWARE OUTPUT.txt
{3F35F070-99D6-11D2-8D10-00A0C9441E20}  Audio Repackager
{3f454f0e-42ae-4d7c-8ea3-328250d6e272}  Automation context menu
{3F4DACA4-160D-11D2-A8E9-00104B365C9F}  VBScript Regular Expression
{3F66389B-BA65-4782-BA9D-B66367C8E7F1}  Power Control Panel
{3F66CF3F-68BE-485e-8BFE-0A005B2D00F2}  Setting Unit Factory
{3F6953F0-5359-47FC-BD99-9F2CB95A62FD}  Personal Start Menu
{3F69F351-0379-11D2-A484-00C04F8EFB69}  CrIris
{3f6bc534-dfa1-4ab4-ae54-ef25a74e0107}  System Restore
{3F9A55B0-8355-4CE4-B6D6-A65CAC63DB67}  CellularAPI
{3fb11ad5-928d-4534-b217-2ffbfdbb6395}  Microsoft Shared Correction UI
{3FBA60A6-7BF5-4868-A2CA-6623B3DFFEA6}  Automatic Maintenance task to enable
Windows Search to make progress while in Connected Standby
{3FC0B520-68A9-11D0-8D77-00C04FD70822}  Display Control Panel HTML Extensions
{3fd7f233-a716-472e-8f2f-c25954f34e96}  AudioFormatConvert Class
{3FECE929-9E54-42D2-A598-82A7C6D7B511}  Tile Management Factory
{3FF23902-CD1F-11D2-8853-0000F80883E3}
{3FF292B6-B204-11CF-8D23-00AA005FFE58}  FoxOLEDB 1.0 Object
{3FF566F0-6E6B-49D4-96E6-B78886692C62}
{3FFB3B8C-EB99-472b-8902-E1C1B05F07CF}  LPCM Byte Stream Handler
{4000C97B-791B-425F-9AD6-5046210503B1}  SpCommunicator Class
{4003191F-71FF-49A2-B591-05C606FADB8B}  WMPlayer MusicPropPage Class
{40036581-8ff3-4cec-bd86-fe9593832546}  Desktop Switch Manager
{4020D514-E884-42E9-91DC-E1F09004D3F0}  CLSID_SoftLandingManager
{40319fab-cc2f-4cea-890c-1e676b139824}  CBasicPropertiesProxy
{40419485-C444-4567-851A-2DD7BFA1684D}  Phone and Modem Control Panel
{4044e60c-7b01-4671-a97c-04e0210a07a5}
{404A6DE5-D4D6-4260-9BC7-5A6CBD882432}
{405EC9AB-0C64-4B9F-B726-3A858A9E2BD6}  Immersive App Crusher
{40871C59-AB40-471F-8DC3-1F259D862479}  MPEG2 Byte Stream Handler
{40AFA0B6-3B2F-4654-8C3F-161DE85CF80E}  Connected User Store
{40B47A8F-C442-4f06-8304-AA1058EDEEA0}  CLSID_POSyncServices
{40dd6e20-7c17-11ce-a804-00aa003ca9f6}  Shell extensions for sharing
{40F5CB5E-86D7-4378-A87C-CE06448EF6B2}  DeviceBroker_PSFactory
{410381DB-AF42-11D1-8F10-00C04FC2C17B}  COMNSView Class
{41070793-59E4-479A-A1F7-954ADC2EF5FC}
{4125dd96-e03a-4103-8f70-e0597d803b9c}  Microsoft Attachment Services
{41445657-4118-4689-B300-E7F1EB61FF7B}  MTF Suggestion InputQuery
{41457294-644C-4298-A28A-BD69F2C0CF3B}  ASF Byte Stream Handler
{414ac301-8d95-43c8-99d0-3f25e4076945}  Microsoft Shared Correction UI
{4150F050-BB6F-11D0-AFB9-00AA00B67A42}  Format
{418008F3-CF67-4668-9628-10DC52BE1D08}  BDA Tuning Model MPEG2 Component Type
Class (Broadcast Substream Type)
{418AFB70-F8B8-11CE-AAC6-0020AF0B99A3}  Quality Management Property Page
{418c8b64-5463-461d-88e0-75e2afa3c6fa}  Explorer Browser Results Folder
{41937347-2aba-4d4c-a4ca-6fe4f11f1bac}  Network Item Factory
{41B23C28-488E-4E5C-ACE2-BB0BBABE99E8}  HHCtrl Object
{41B89B6B-9399-11D2-9623-00C04F8EE628}  SpInprocRecognizer Class
{41B9BE05-B3AF-460C-BF0B-2CDD44A093B1}  XML filter
{41CA099A-B8AF-4fc2-A285-03FAEAA8B109}  TypeAhead Framework
{41E300E0-78B6-11ce-849B-444553540000}  Display Effects CPL Extension
{41FCCC3A-1FA1-4949-953A-6EE61C46A4D1}  Microsoft.Audio.AudioClient Binder
{42044394-8c34-11d1-83bc-00c04fbbc34e}
{42060D27-CA53-41f5-96E4-B1E8169308A6}  ReliabilityAnalysisCustomHandler
{42071712-76d4-11d1-8b24-00a0c9068ff3}  Display Adapter CPL Extension
{42071713-76d4-11d1-8b24-00a0c9068ff3}  Display Monitor CPL Extension
{420A51A3-D605-430C-B4FC-45274FA6C562}  Microsoft H265 Video Decoder MFT
{42150CD9-CA9A-4EA5-9939-30EE037F6E74}  Microsoft MPEG-2 Video Encoder
{421516C1-3CF8-11D2-952A-00C04FA34F05}  Chroma
{42281387-EDEA-477C-89DB-6F7033D518AB}  Notify Local Setting Change
{4234d49b-0245-4df3-b780-3893943456e1}  Applications
{42393E99-8513-42d3-8AEA-E0E5FBDC8F64}  User Name XML
{424B71AF-0695-11D2-A484-00C04F8EFB69}  CrRadialWipe
{424bed78-ef88-4b7c-945c-b8cf46d56e20}  Authentication UI Last Logged On Username
                              Page 51
```

SOFTWARE OUTPUT.txt

```
{426C82B9-D74C-4873-BC90-28FC7BE0A32A}  Bitmap Result Object
{4278BB8C-D0FC-4380-A2C4-525B9A396F5B}  TypeAhead Search History Provider
{427B34A5-2199-467e-BAC2-112AC1A48391}  NarratorMenuItem Class
{427BC7E3-F833-4584-8745-CFAB9D7A5761}  CTaskConditionCombiner
{4290CAD6-A75D-4AC8-A496-56DBBB28EB88}  User Tile Setting Monitor
{429AF92C-A51F-11d2-861E-00C04FA35C89}  %Trident API%
{429bc048-379e-45e0-80e4-eb1977941b5c}
{42aedc87-2188-41fd-b9a3-0c966feabec1}  MruPidlList
{42C21DF5-FB58-4102-90E9-96A213DC7CE8}  EntAppSvc
{42C9B9F5-16FC-47ef-AF22-DA05F7C842E3}  WAV Byte Stream Handler
{42CBFAA7-A4A7-47BB-B422-BD10E9D02700}  Diagnostics Hub Standard Collector Service
{42DFB618-A403-4401-908F-FE979B2215C8}  PSFactoryBuffer
{42FEBF74-65EA-4D27-B3AC-86393B6AFAE1}  Search Query Services
{430da762-8632-4840-bc61-3eeaa078e62e}  Windows Display Settings Data
{43136EB5-D36C-11CF-ADBC-00AA00A80033}  NodeInit 1.0 Object
{4315D437-5B8C-11D0-BD3B-00A0C911CE86}  DeviceMoniker
{43232233-8338-4658-ae01-0b4ae830b6b0}  Portable Device IDispatch Factory
{4323664B-B884-4929-8377-D2FD097F7BD3}  PSFactoryBuffer
{43324B33-A78F-480F-9111-9638AACCC832}
{4333fd20-ca5f-4095-a535-edb00455ce66}  File Input Stream Marshaller
{4336a54d-038b-4685-ab02-99bb52d3fb8b}  Public Folder
{434A6274-C539-4E99-88FC-44206D942775}  AccesibilityCplAdmin Class
{4356b08e-ecb5-43d1-8e9f-7bef4fc960fe}  Manage Add-ons Admin Broker
{435899C9-44AB-11D1-AF00-080036234103}  DSPrintQueue Class
{437ff9c0-a07f-4fa0-af80-84b6c6440a16}  Command Folder
{43886CD5-6529-41c4-A707-7B3C92C05E68}  IE Navigation Bar
{43A1BB0E-2CE9-405C-8799-12E7D7550D3F}  Raw Input Provider
{43A8F463-4222-11d2-B641-006097DF5BD4}  Shell Name Space ListView
{43B07326-AAE0-4B62-A83D-5FD768B7353C}  InkRectangle Class
{43C103A6-696F-4D05-AF04-9E44A6844B30}  OOBE Timezone UI Module
{43D7FDB4-B94D-4415-8792-54AF9FBEBB82}  Microsoft Transition Technologies WMI
Provider
{43FB1553-AD74-4ee8-88E4-3E6DAAC915DB}  InkCollector Class
{4405b37b-60fe-49ed-ba8f-691a78f84daf}
{44090B31-CDF9-4ad1-8182-DB5DA3627974}  SystemSettings Application Execute Open
Verb
{44121072-A222-48f2-A58A-6D9AD51EBBE9}
{44185ED5-CB6F-46C4-AB1F-31A2694C2760}  PhoneLauncherService
{442FF639-3DA0-4A70-A1D8-579E26C46A60}  PS Module Discovery Provider
{443C8934-90FF-48ED-BCDE-26F5C7450042}  PSFactoryBuffer
{443E7B79-DE31-11D2-B340-00104BCC4B4A}  WbemUnauthenticatedLocator Class
{4444AC9E-242E-471B-A3C7-45DCD46352BC}  VMR Allocator Presenter DDXcl Mode
{447EDBE5-0080-4036-A0BB-7B84C58C604F}  IEDataObjectWrapper
{44838BA6-68C6-4951-8CD5-1DD1B4787B53}
{4487FB5A-9D22-4718-AA9F-C6ED6C4EC169}  NarratorSuperBar Class
{4489A5C2-F662-47FC-A733-B3577E162DF7}  SystemAudioDeviceSharedNew Class
{448aee3b-dc65-4af6-bf5f-dce86d62b6c7}  Property sheet handler
{44A50F5F-78E2-4D17-930C-68BB9F69EC9E}  Immersive Launcher
{44BAF61B-E481-4305-9166-33B1FD3F4876}  Credential Migration Handler
{44C76ECD-F7FA-411c-9929-1B77BA77F524}  IE Menu Site
{44CB442B-9DA9-49df-B3FD-023777B16E50}  Http Scheme Handler
{44da8435-b187-4dd6-8f32-9341eb7e4c3c}  CLSID_CSmapiProxy
{44EC053A-400F-11D0-9DCD-00A0C90391D3}  Registrar Class
{44f3dab6-4392-4186-bb7b-6282ccb7a9f6}  MyDocuments menu and properties
{44F9A03B-A3EC-4F3B-9364-08E0007F21DF}  TaskSymbol Class
{450D8FBA-AD25-11D0-98A8-0800361B1103}
{451256BC-E7E8-4506-90F3-8746E107BF08}  NarratorTitleBar Class
{4522c772-9a2b-4920-ad7f-62d3d15eac52}  Restore Default Favorite Links Command
{45234E3E-61CC-4311-A3AB-248082554482}  Plug-in Terminal
{452eee0c-a2d4-49c3-9f19-1493e7709220}  PIN Logon Enrollment UX
{4545dea0-2dfc-4906-a728-6d986ba399a9}  Thumbnail Extraction Host Class
{454AFB66-FA8C-4152-9CD6-2A8781B3D505}
Windows.ApplicationModel.Chat.RcsEndUserMessageAvailableTriggerDetails Factory
```

Page 52

SOFTWARE OUTPUT.txt

```
{45597c98-80f6-4549-84ff-752cf55e2d29}    Add to Windows Media Player list
{455ACF57-5345-11D2-99CF-00C04F797BC9}    PSFactoryBuffer
{455F24E9-7396-4A16-9715-7C0FDBE3EFE3}    SpNullPhoneConverter Class
{455f6102-c83a-4d07-ba36-b6da9d589ae2}    RdpAudioSink Class
{4564b25e-30cd-4787-82ba-39e73a750b14}    Recent Items Instance Folder
{45670FA8-ED97-4F44-BC93-305082590BFB}    Microsoft XPS Shell Metadata Handler
{4582746F-473B-4022-A7E9-887CBEDD8F85}    SBE IO counters
{4582EBA9-6AA1-4D79-824E-728929EF455D}    HomeGroup Task
{45874AC3-B98F-4851-9046-5CFE1E747DD4}    NarratorSeparator Class
{4590F811-1D3A-11D0-891F-00AA004B2E24}    WBEM Locator
{4590F812-1D3A-11D0-891F-00AA004B2E24}    Microsoft WBEM WbemClassObject Marshalling
proxy
{45BA127D-10A8-46EA-8AB7-56EA9078943C}    Application Activation Manager
{45C8FAEC-0447-4BD7-A09E-A91BFF9AB53C}    UsoSession
{45FB4600-E6E8-4928-B25E-50476FF79425}    Com Call Wrapper Unmarshal Class 4.0
{45FD65ED-6BC2-47ae-B391-9E2B79F07C52}    System Control Panel
{45ffc283-e417-4bc2-b0b8-6654081d10d7}    Pin Enrollment Singleton
{46031ba1-083f-47d9-8369-23c92bdab2ff}    AC-3 Byte Stream Handler
{461CDD3F-D54E-4033-A0AA-6CD24F152AA1}    WlanDlg Get Key UI Page Class
{461DED9E-81D5-494F-BC96-6432C8645733}    SpObjectTokenCategory Class
{464510d9-3477-4c8b-97cb-4b4c29f04354}    ICastServerAppRegistrar Factory
{4654B883-10C0-4524-96B6-7D997104DCF0}    SystemAudioDeviceOffload Class
{4655840e-ab1a-49d0-a4c4-261fa1c20e86}    Windows Push Notification Platform Class
Factory
{4657278A-411B-11d2-839A-00C04FD918D0}    Shell Drag and Drop helper
{4661626C-9F41-40A9-B3F5-5580E80CB347}    tiledatamodelsvc
{4662DAA5-D393-11D0-9A56-00C04FB68BF7}
{4662DAA6-D393-11D0-9A56-00C04FB68BF7}
{4662DAA7-D393-11D0-9A56-00C04FB68BF7}
{4662DAA8-D393-11D0-9A56-00C04FB68BF7}
{4662DAA9-D393-11D0-9A56-00C04FB68BF7}
{4662DAAA-D393-11D0-9A56-00C04FB68BF7}
{4662DAAB-D393-11D0-9A56-00C04FB68BF7}
{4662DAAC-D393-11D0-9A56-00C04FB68BF7}
{4662DAAD-D393-11D0-9A56-00C04FB68BF7}
{4662DAAE-D393-11D0-9A56-00C04FB68BF7}
{4662DAAF-D393-11D0-9A56-00C04FB68BF7}
{4662DAB0-D393-11D0-9A56-00C04FB68B66}
{4662DAB0-D393-11D0-9A56-00C04FB68BF7}
{466936A9-E281-45E6-A239-9FE53D07B4A5}    Lock Screen Slideshow Feed Manager
{46763EE0-CAB2-11CE-8C20-00AA0051E5D4}    Obsolete Font
{469afbdf-084f-4dc9-904f-9e824c48bc37}    Folder Initialization Handler
{46A4DD5C-73F8-4304-94DF-308F760974F4}    Microsoft MPEG-2 Audio Encoder MFT
{46b73c9c-0e62-41ee-86c0-2f8997777f48}    Microsoft IME (Japanese) IFELang
{46C166AA-3108-11D4-9348-00C04F8EEB71}    Home Networking Configuration Manager
{46CF315B-2D3A-4765-852A-6500C42D9865}    TypeAhead Search History Settings
{4705A6B4-E4CB-4ed1-AF8D-851C644A0459}    Select None command invocation
{470C0EBD-5D73-4d58-9CED-E91E22E23282}    Pin To Start Screen verb handler
{47135eea-06b6-4452-8787-4a187c64a47e}    SdrRestoreService Class
{47206204-5ECA-11D2-960F-00C04F8EE628}    SpSharedRecoContext Class
{4729BA91-6337-4013-A5DC-BB9EBFDA2B04}    DataPackageHostEventDetails
{47354492-827E-4b8a-B318-C80EBA1381F0}    CClusterDetectorEX
{4738383A-B2E1-44e2-9B24-412FE1D0E843}    Content Tile Monitor Callback
{473AA80B-4577-11D1-81A8-0000F87557DB}    DX2D Anti-Aliasing
{47405ACE-008F-43AB-B6F0-91875029ADC7}    Work Folders Launch Sync Status Action
{4753da60-5b71-11cf-b035-00aa006e0975}    ADs Provider Object
{475743C2-3495-4FD5-B23D-CB36CF813D19}    MCCSSmtpSyncEngine
{477EC299-1421-4bdd-971F-7CCB933F21AD}    File Scheme Handler
{478B7068-DF14-446F-B5C1-A5B877E7665D}    PSFactoryBuffer
{47B706B0-B103-4AFD-8ECF-16C2DDF81C15}    Microsoft Network Connectivity WMI
Provider
{47B73B70-1964-444A-B390-FAB1565DCAA3}    SpNotifyTranslator Class
{47D35BB4-71CC-4810-9669-D03D9FF7CEAF}    DDRCPropertySource Class
```

Page 53

SOFTWARE OUTPUT.txt

```
{47D4D946-62E8-11cf-93BC-444553540000}   DirectSound Object
{47DFBE54-CF76-11D3-B38F-00105A1F473A}   WBEM Scripting DateTime
{47e30d54-dac1-473a-aff7-2355bf78881f}   NGC Pregeneration Task Handler
{48025243-2D39-11CE-875D-00608CB78066}   Internal Text Renderer
{480FF4B0-28B2-11D1-BEF7-00C04FBF8FEF}   DirectMusicCollection
{48123BC4-99D9-11D1-A6B3-00C04FD91555}   XML Document
{483afb5d-70df-4e16-abdc-a1de4d015a3e}   AzPrincipalLocator Class
{4844E347-E354-4B24-9E0C-F4AE31AD55DB}   XblAuthTokenResult
{48527bb3-e8de-450b-8910-8c4099cb8624}   Empty Recycle Bin verb invocation
{4876DC0E-F963-4227-9A8F-19872B75D231}   Storage Devices Handler
{48794782-6a1f-47b9-bd52-1d5f95d49c1b}   Device Installation Reboot Dialog Task
{487af411-1d5e-4f7f-b4f4-4721fe1e95d9}   CVideoPropertiesProxy
{488A2E25-B509-4238-97BA-CAB956F8C2F5}   SmMessage
{488C2839-8ABA-4368-B4DF-8EF11CF99F99}   MSASR Locale Handler Class (General)
{489331DC-F5E0-4528-9FDA-45331BF4A571}   CInitiateWinSAT Class
{489AE5DA-059A-4aca-93E5-7B7CFD1BD752}   BOOTSTRAP.1.0
{48d7ed61-3f9f-4d74-8c2f-a10541d4151d}   ImePhoneticConversionJpn
{48da6741-1bf0-4a44-8325-293086c79077}
{48DE828C-730C-49AF-AE84-759C609911EE}
{48E277F6-4E74-4cd6-BA6F-FA4F42898223}   Windows Search OpenSearch Provider
{48e2ed0f-98c2-4a37-bed5-166312ddd83f}   MFReadWrite Class Factory
{48e7caab-b918-4e58-a94d-505519c795dc}   Start Menu Folder
{49010C18-B110-421a-9047-ADCA421CBC40}   IMRequestRA Class
{4933656C-55E2-48e6-AD89-679CAE6295DF}   Marshal-By-Value Ref Counted Event
{4955DD33-B159-11D0-8FCF-00AA006BCC59}   CActiveIMMApp
{496241E9-161B-4007-AF56-B4E006F65FA9}
{49638B91-48AB-48B7-A47A-7D0E75A08EDE}   BDA Tuning Model Analog Locator
{497D141A-7A42-4BB6-B017-863FD4DA36BF}
{4988dd22-ccec-48ec-9271-5951e8653903}   TTLS Non EAP Interactive UI class
{498B0949-BBE9-4072-98BE-6CCAEB79DC6F}   SmartRenderEngine Class
{4991d34b-80a1-4291-83b6-3328366b9097}   Background Intelligent Transfer Control
Class 1.0
{499EAEEA-2737-4849-8BB6-47F107EAF358}   CTocParser
{49A832D7-C7B3-4556-8716-5BDC745C3C1B}   BackupSettings
{49ACAA99-F009-4524-9D2A-D751C9A38F60}   PSFactoryBuffer
{49B2791A-B1AE-4C90-9B8E-E860BA07F889}   MMC Application Class
{49BD2028-1523-11D1-AD79-00C04FD8FDFF}   Microsoft WBEM Unsecured Apartment
{49BD2BB3-DFBE-4E01-BF21-7DE89ED09ACD}
{49C407EF-78B9-4C82-A40B-2FE02F8E771D}   Windows Theme Thumbnail Preview
{49c47ce0-9ba4-11d0-8212-00c04fc32c45}   SFilter Class
{49C47CE4-9BA4-11D0-8212-00C04FC32C45}   Stream Class
{49c47ce5-9ba4-11d0-8212-00c04fc32c45}   MMStream Class
{49E9AE53-4547-4045-AAD1-CDC3C6C95D6C}   PSFactoryBuffer
{49eb6558-c09c-46dc-8668-1f848c290d0b}   Scope Picking Dialog
{49f171dd-b51a-40d3-9a6c-52d674cc729d}   UIAutomationCrossBitnessHook64 Class
{49F371E1-8C5C-4d9c-9A3B-54A6827F513C}   Sharing Configuration Manager
{4A03DCB9-6E17-4A39-8845-4EE7DC5331A5}   Spiral
{4a04656d-52aa-49de-8a09-cb178760e748}   Recycle Bin Manager
{4A16043F-676D-11d2-994E-00C04FA309D4}   CLSID_DatabaseSession
{4A1E5ACD-A108-4100-9E26-D2FAFA1BA486}   IGD Property Page
{4A2286E0-7BEF-11CE-9BD9-0000E202599C}   MPEG Audio Codec
{4A38E4EF-F55B-4A59-8F02-BDEFB0B1308A}   CGNPMpeg2DataControl
{4a4d5d1b-869b-4474-806a-4daaa7673e78}
{4A4EBE8E-AE27-4AA3-B702-F365C4A90FAC}   PSFactoryBuffer
{4A5869CF-929D-4040-AE03-FCAFC5B9CD42}   Generic Sink Segment
{4A65D267-1539-4BD1-921D-1C49B3E58EB7}   SnapInFailureReporter
{4A6B8BAD-9872-4525-A812-71A52367DC17}   RasGcw LUA
{4a714c8e-e664-4024-9c74-1a82a3da842a}   Authentication UI Background
{4a76b469-7b66-4dd4-ba2d-ddf244c766dc}   GSM ACM Wrapper MFT
{4a7ded0a-ad25-11d0-98a8-0800361b1103}   MyFolder menu and properties
{4AA0A5C4-1B9B-4F2E-99D7-99C6AEC83474}   Setting Sync Task
{4AA53027-562B-4653-A8EF-9B92FF74ADA6}   Windows.Devices.Bluetooth Proxy
{4ABF5A06-5568-4834-BEE3-327A6D95A685}   Matrix
```

Page 54

SOFTWARE OUTPUT.txt

```
{4ac6c205-2853-4bf5-b47c-919a42a48a16}  Show File Extensions Explorer Command
{4AF3D182-65F6-401E-B0A8-02B5928D77CA}  EA Physical Keyboard Skin Class
{4AF3F4A4-06C8-4B79-A523-633CC65CE297}  WBEM Disk Quota Volume Provider
{4AF4A5FC-912A-11D1-B945-00A0C90312E1}  Microsoft Docking Bar Property Bag
{4B181F0F-48C8-4e80-A2AF-E3099AAC069B}  PresentationHost in-proc handler
{4B2E958D-0393-11D1-B1AB-00AA00BA3258}  COM+ Active Process Iteration Server
{4B314A47-12E0-4d52-95FE-084B9224DD4F}  WmiProfileAssociation
{4B534112-3AF6-4697-A77C-D62CE9B9E7CF}  Sync Center Event Properties Extension
{4B59AFCC-B8C3-408A-B670-89E5FAB6FDA7}
{4b6657e4-b973-46cd-9bb3-6e5ebd82448f}  PortableDeviceWMDRM Class
{4B6C85F1-A6D9-433A-9789-89EA153626ED}  tiledatamodelsvc
{4b77066b-8a60-4162-9456-1b1e994eaf77}  CloudExperienceHost Defalut Admin
Elevation Broker Manager
{4B78D326-D922-44f9-AF2A-07805C2A3560}  IE Menu Band
{4B905E0F-8E31-4853-BA9F-9BE581A35535}  Windows.UI.Input.InjectionBroker
{4B966436-6781-4906-8035-9AF94B32C3F7}  SPP Class
{4BB24BC2-ABFD-433D-935F-5950B42A4B3F}  Immersive Session Idle Detector
{4BC67F23-D805-4384-BCA3-6F1EDFF50E2C}  ERCLuaElevationHelper
{4bc70a10-fbab-4ada-8fc4-e4f898a6f810}  CImagePropertiesProxy
{4BCCBCE4-20E8-44A1-A170-C9A4D941CBA4}  DNS Client Configuration WMI/PowerShell
Provider
{4BDAFC52-FE6A-11d2-93F8-00105A11164A}  IVolumeClient2_PSFactory
{4BDD6232-2E55-4A1F-AAAD-961D76F439BA}  PSFactoryBuffer
{4be5c3b3-53a2-4f2f-af9d-d26a5327eb92}  Microsoft Korean IME 9.0 SKF Applet
{4bec2015-bfa1-42fa-9c0c-59431bbe880e}  Shell URL
{4C1D33D1-3161-4A76-9487-2677CD589C11}
{4C1FC63A-695C-47E8-A339-1A194BE3D0B8}  UIAnimationManager
{4c2b3015-779e-421c-b54a-b8d5659e880a}  HttpRequest
{4C34A351-5CEC-47A5-8252-075D403C7BF6}  Backstack settings change notify callback
handler
{4C3624D8-57AF-11E1-B779-E5CC4724019B}  Theme Setting Handler
{4C3E5154-0E70-4C0C-9EDC-08277E8F163A}  ProvPluginEngine
{4C4A5E40-732C-11D0-8816-00A0C903B83C}  CertServerPolicy Class
{4C596AEC-8544-4082-BA9F-EB0A7D8E65C6}  CivicAddress Report Class
{4C5EBD71-431C-43A0-B93C-3EBF917B540F}  File System Setting Change Publisher
{4C5EF749-A380-44FE-853D-FF928F2CD1AE}  Immersive Shell Tracing Service
{4C60517F-C1F8-473A-B1D8-247952876A5A}  Roaming Options Values
{4C6470A6-3F91-4f41-850B-DB9BCD074537}  Microsoft Feeds Background Sync Component
{4c649c49-c48f-4222-9a0d-cbbf4231221d}  Photo Printing with Templates Wizard
{4C6F940C-3CFE-11D2-9EE7-00C04F797396}  SpTaskManager Class
{4c870c20-4ed3-4235-9a2a-7185f8a87d06}  HanjaDic Class
{4c892621-6757-4fe0-ad8c-a6301be7fba2}  Windows Settings Page
{4C8CC9CB-80CA-4e16-9F60-F5EB55092361}  Send Search to Computer Command
{4C8D0AF0-7BF0-4f33-9117-981A33DBD4E6}  FilePlaybackTerminal Class
{4c9ba57a-e8eb-49db-ba55-811b3e1358b4}
{4cadfae1-5512-456a-9d65-5b5e7e9ca9a3}  Provides customized initialization for WPD
drivers using IPortableDeviceClassExtension
{4CB26C03-FF93-11d0-817E-0000F87557DB}  DXTaskManager
{4CBE39A3-BD8A-4D51-9BD3-B7853737FD93}  CLSID_SplashScreenInfo
{4CCEA634-FBE0-11d1-906A-00C04FD9189D}  Pixelate
{4cd0569b-0239-4602-84a3-cfc5a9167c82}  Cloud Experience Host CLSID_Elevation
Broker Context
{4CDC41C7-C20F-4163-992D-10AC7FBF0BE3}  LockScreen Toast Notification Status
Provider
{4ce6767d-e09b-45dc-831d-20c8b4ea9a26}  Open With command
{4CFC7932-0F9D-4BEF-9C32-8EA2A6B56FCB}  Microsoft WMI Provider Subsystem Decoupled
Registrar
{4D111E08-CBF7-4f12-A926-2C7920AF52FC}  Shell Security Editor
{4d233817-b456-4e75-83d2-b17dec544d12}  Background Intelligent Transfer Control
Class 10.0
{4D317113-C6EC-406A-9C61-20E891BC37F7}  RASettingProperty Class
{4D3BD4B7-AD22-4DC4-B889-311DAE0D8AEB}  WindowServerFactory
{4d4dedaa-43c5-480d-9ee0-1464f9f4ff4b}  MF SVR Activate
```

Page 55

SOFTWARE OUTPUT.txt

```
{4d56df98-e082-4bf4-9a09-df655d8427b6}  Multitasking View
{4D5C8C2A-D075-11d0-B416-00C04FB90376}  Microsoft CommBand
{4D728E35-16FA-4320-9E8B-BFD7100A8846}  FhReassociation Class
{4DB1AD10-3391-11D2-9A33-00C04FA36145}  PSFactoryBuffer
{4db26476-6787-4046-b836-e8412a9e8a27}  Shared Bitmap Object
{4DB61F89-EECE-4317-89D2-EC17BF6B27DB}  NarratorScrollBar Class
{4DC9C264-730E-4CF6-8374-70F079E4F82B}  Windows To Go Shell Service Object
{4DD1D1C3-B36A-4eb4-AAEF-815891A58A30}  Vector Class
{4DD441AD-526D-4A77-9F1B-9841ED802FB0}  SAXAttributes
{4DDA1941-77A0-4fb1-A518-E2185041D70C}  CTocGeneratorDmo
{4DDB6D36-3BC1-11d2-86F2-006008B0E5D2}  MSP Class
{4DE225BF-CF59-4CFC-85F7-68B90F185355}  Microsoft WMI Provider Subsystem
{4de7016c-5ef9-11d1-8c13-00c04fd8d503}  Microsoft User Extension
{4df0c730-df9d-4ae3-9153-aa6b82e9795a}  Known Folder Manager
{4DF929E7-4C5E-4587-A598-7ED7B3D6E462}  AddMdmObj Class
{4DFED3F9-B794-4d3c-973B-DDA1C28105A9}  Private Profile Object
{4E0680A0-A0A2-11D0-8821-00A0C903B83C}  Encode Long Array Class
{4E14FBA2-2E22-11D1-9964-00C04FBBB345}  Event System
{4E3073AC-CE55-B07D-A284-1641E2236DDA}  Windows.Networking.Vpn.ProxyStubFactory
{4e3c6645-b839-4a06-a27b-0190f9e6a0af}  Synchronous IAM Event Handler (global)
{4E40F770-369C-11d0-8922-00A024AB2DBB}  Security Shell Extension
{4E7D6B2C-1F7E-45B6-9EC0-8FA541BDD163}  Per User Initialization Task Handler
{4ea9a1b7-e521-4813-a9f8-ba6484902cb5}  SMB Helper Class
{4eb2f086-c818-447e-b32c-c51ce2b30d31}  Microsoft RDP Client Control - version 6
{4EB31670-9FC6-11CF-AF6E-00AA00B67A42}  DV Splitter
{4eb89ff4-7f78-4a0f-8b8d-2bf02e94e4b2}  Microsoft RDP Client Control
(redistributable) - version 6
{4ED3A719-CEA8-4BD9-910D-E252F997AFC2}  Association Launch Execute Command
{4EDCB26C-D24C-4e72-AF07-B576699AC0DE}  Microsoft RDP Client Control
(redistributable) - version 5
{4EDD6725-7003-4120-A0BB-BBDEBA704FB7}  LockAppHost Out of Proc Server for Lock
Apps
{4F1DFCA6-3AAD-48E1-8406-4BC21A501D7C}  Workspace Class
{4F23C296-F56E-45AF-904D-D245BF750759}  Sync Command Gallery
{4f37e3a9-1d2b-42ab-a5b0-31fc05627def}  Shell Feedback Service
{4F414126-DFE3-4629-99EE-797978317EAD}  SpPhoneticAlphabetConverter Class
{4F4DB904-CA35-4A3A-90AF-C9D8BE7532AC}  RecoExt Class
{4F4DD15E-F431-4536-AEE8-AF20BA847A33}  SpNullPhoneConverter Class
{4F58F63F-244B-4c07-B29F-210BE59BE9B4}  .group shell extension handler
{4F664F91-FF01-11D0-8AED-00C04FD7B597}  OleSNMP Class
{4f6bcd94-c2a5-42ce-8dbc-31e794be4630}  Shell Computer Accounts
{4F786E23-0F32-4888-BA02-6BB105AE3024}  SpWASAudioIn Class
{4f7d48de-1045-48b0-adba-f0b6d93a18f4}  PIN Logon Enrollment Handler
{4f8e67d6-de03-480b-80aa-52f9c1aeffea}
{4FA18276-912A-11D1-AD9B-00C04FD8FDFF}  InProcWbemLevel1Login Class
{4fab6371-6d65-47ba-b8f1-ca6273c6c69e}  Sort Groups Ascending Explorer Command
{4FB1CE6D-5334-414A-BBBC-F892A47587E3}
{4FD2A832-86C8-11D0-8FCA-00C04FD9189D}
{4FDBC3E5-7121-4487-AB95-B58EC04648DB}  Extensible Media Manager Helper Class
{4FDEF69C-DBC9-454e-9910-B34F3C64B510}  PSFactoryBuffer
{4FE24495-28CE-4920-A4C4-E556E1F0DF2A}  CToc
{4fe2776b-b0f9-4396-b5fc-e9d4cf1ec195}  ImePlugInDictDictionaryList_JPN Class
{4FF2FE0E-E74A-4B71-98C4-AB7DC16707BA}
{4FF787E6-9A86-4BA3-BED9-8019A2B4BE1C}  Input Host Layout
{4FFFD315-B178-46E5-A386-A45C7AFF4154}  Windows.Help.Runtime.Catalog
{5002C79D-2459-4797-B9F4-7438A2BF818D}
{50040C1D-BDBF-4924-B873-F14D6C5BFD66}  MediaDevMgrClassFactory Class
{50055B2F-D4FF-42E1-9D8F-5D48F327F3AC}  WERCOM
{500DD1A1-B32A-4a37-9283-1185FB613899}  PSFactoryBuffer
{5014B7C8-934E-4262-9816-887FA745A6C4}  TPM Maintenance Task Handler
{503E9FD4-127C-4d72-84BF-CF3EC3F80D40}  File Placeholder Handler
{505734c0-686d-456a-9cb3-c666cbda5972}  NarratorThread Class
{5058292D-A244-4840-AB44-480975C4FFE4}  CTocCollection
```

Page 56

SOFTWARE OUTPUT.txt

```
{50613c35-8120-4721-849e-2df54d82cc33}  ImeLmTestJpn
{506229ae-09c7-4ffd-8ec9-6a957f6da601}  Library Public Save Location verb
{506D89AE-909A-44f7-9444-ABD575896E35}  DxtAlphaSetter Class
{5088B39A-29B4-4d9d-8245-4EE289222F66}  QueryParserManager Class
{50A41EF1-6BFA-4b7e-973E-798EA0BEBAD4}  ConfigManager2URI
{50B1904B-F28F-4574-93F4-0BADE82C69E9}
{50B6327F-AFD1-11d2-9CB9-0000F87A369E}  AD System Info Object
{50D42F09-ECD1-4B41-B65D-DA1FDAA75663}
{50D5107A-D278-4871-8989-F4CEAAF59CFC}  CActiveIMMAppEx_Trident
{50EF4544-AC9F-4A8E-B21B-8A26180DB13F}  Local Thumbnail Cache
{50FDBB99-5C92-495E-9E81-E2C2F48CDDAE}  Immersive Application Manager
{50ff05d3-62ae-402b-9b06-3cf57f74c9dc}  PlayToReceiver
{510C4E33-05D5-438B-9852-E8406EFF033D}  PSFactoryBuffer
{51208789-BD2C-475E-8265-438DFBF78F9C}  ElementSelectedEvent Class
{51372af3-cae7-11cf-be81-00aa00a2fa25}  MTSPackage
{513a0312-3345-4d16-94e5-630b0262c2eb}  CLSID_HostedApplicationActivationManager
{513D916F-2A8E-4F51-AEAB-0CBC76FB1AF8}  LayerUIPropPage
{514B5E31-5596-422F-BE58-D804464683B5}  Region and Language UAC Elevation
{51571744-7FE4-4FF2-A498-2DC34FF74F1B}  MediaVideoStabilizationEffect
{515980c3-57fe-4c1e-a561-730dd256ab98}  Desktop Status Service
{5160F343-7A1F-46C2-9E21-FC7F1DAF37F3}  Browser Favorites File System Monitor
Callback
{51648e7c-d7b2-449c-b513-46050dcfd917}  IHV page launcher task Class
{51653423-E62D-4FF7-894A-DABB2B8E21E2}  CrawlStartPages Task Handler
{5167B42F-C111-47A1-ACC4-8EABE61B0B54}
{517F6AA6-D6FA-46D0-8094-17FF17E4CCF4}  HomeGroup Security Hosted Listener
{51a1467f-96a2-4b1c-9632-4b4d950fe216}  Shell Disc Image Mount
{51ad6d44-32f8-4aa7-9ee6-24a37fa09354}
{51B4ABF3-748F-4E3B-A276-C828330E926A}  Video Mixing Renderer 9
{51C0B2CF-5994-4c2c-93F1-1C2CE21DFF4B}  NarratorTreeView Class
{51CAFEF2-C040-4022-A152-53033EE9A02B}  Sync root make available offline verb
{51CEDF03-4316-47C9-8100-CAC54EC2E33F}  AsyncContentLoadedEvent Class
{51D1268C-D0A5-47CC-A514-547F346F45E8}  Launcher Tip Context Menu
{51F649D3-4BFF-42f6-A253-6D878BE1651D}  User Libraries Setting Handler
{520CCA61-51A5-11D3-9144-00104BA11C5E}  Microsoft IMAPI Disc Recorder
{520CCA63-51A5-11D3-9144-00104BA11C5E}  Microsoft IMAPI Disc Master
{520E9D28-64C4-43df-BEED-02D9A6044A4B}  Device Query Provider Class
{5210f8e4-b0bb-47c3-a8d9-7b2282cc79ed}  WMAPro over S/PDIF DMO
{52205fd8-5dfb-447d-801a-d0b52f2e83e1}  @%SystemRoot%\system32\shell32.dll,-22067
{5220cb21-c88d-11cf-b347-00aa00a28331}  Microsoft Licensed Class Manager 1.0
{522e34a4-07f7-40a1-94d0-1bfe832efc3a}  PSFactoryBuffer
{524B13ED-2E57-40B8-B801-5FA35122EB5C}  DrawAttrs Class
{524b350e-a28a-425d-a472-c9e2e2c87bfd}
{52550DE3-15E4-4B53-9670-74FCF2B9EA21}  Input Personalization Setting Handler
{5255EFED-103A-4444-B124-F88F99E4EF8D}  HomeGroup Printer Hosted Listener
{525C410E-B007-4F15-81DD-49DF9B17139B}
{5263233A-23CA-4eea-B9A5-25A23EAAF16C}  ActiveSyncAccountAccessor
{527c9a9b-b9a2-44b0-84f9-f0dc11c2bcfb}  Microsoft DocProp Static Property Control
{528d46b3-3a4b-4b13-bf74-d9cbd7306e07}  XML Feed Document
{52968F2C-56B5-4078-9898-EA595DCA0A6E}
{529A9E6B-6587-4F23-AB9E-9C7D683E3C50}  TF_ThreadMgr
{52A2AAAE-085D-4187-97EA-8C30DB990436}  HHCtrl Object
{52B20D0F-167D-4701-9AAF-9E6C3161E735}  NarratorDragPattern Class
{52C84ACA-027A-4536-A74A-E0BB50C44782}  Microsoft iSCSI WMIv2 Provider
{52ce2fe5-04c3-42fd-8a8b-4251affb8408}  CLSID_ResultSetManager
{52F15C89-5A17-48e1-BBCD-46A3F89C7CC2}  LeafCondition Class
{52FEC728-4B3B-4B99-8875-B1E2D16E3D1F}  SQM Listener SSO
{53067330-01CE-4027-947F-FF8580E92463}
{5310BE71-5C14-4FBC-8CF5-BD75D3F11A44}  SpCustomStream Class
{531fdebf-9b4c-4a43-a2aa-960e8fcdc732}  CImeServerCht
{5323BCB5-0431-42be-A482-5EE76F243A28}
{5326dddc-ec38-428d-b219-ce6dadb35de3}  Connect to a network
{53362C64-A296-4F2D-A2F8-FD984D08340B}  RemoteProxyFactory32 Class
```

Page 57

```
                     SOFTWARE OUTPUT.txt
{53445BED-3213-453B-A12A-79AA20A702DC}  LegacyPrintUI Class
{53510d24-57eb-4713-9afb-e6e60530b87e}  IE RSS Feeds Tasks
{535CFF4C-170A-4308-A70E-8188313F3B08}  EvtQProc Class
{536AACFB-5238-4314-B4D4-5B0A2E8B968E}  LockScreenContentServer Out of Proc Helper
for LockScreenContent Clients
{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}  Control Panel command object for Start
menu and desktop
{53a01e9d-61cc-4cb0-83b1-31bc8df63156}  Microsoft DocProp Icon List Control
{53A2A994-97C2-4545-A9CE-0FD6405EA2B2}
{53A36C4F-E620-450B-80B0-4819935BC7F2}
{53bd6b4e-3780-4693-afc3-7161c2f3ee9c}  MruLongList
{53BEDF0B-4E5B-4183-8DC9-B844344FA104}  MAPI Mail Previewer
{53C74826-AB99-4d33-ACA4-3117F51D3788}
{53D6AB1D-2488-11D1-A28C-00C04FB94F17}
{53DEC7F6-5448-43E2-9573-3F7B91B751DC}  DsmDeviceAppCoordinator Class
{53E8EBDD-A50B-46DD-9FAA-42746361EC63}  Lattice Class
{53E9771B-6A21-4FEC-B8F1-3B0DAE4FACC6}  CSpPredictorSet Class
{5408B2F0-C816-11D1-8F99-00600895E7D5}  Interface Proxy Stub
{540D8A8B-1C3F-4E32-8132-530F6A502090}  Language bar
{541987EE-0E02-411E-9A85-1FC6156E7F4B}  audiomatrix class
{54337179-c8b2-4ed4-95e4-95601c850d8c}
{5440837F-4BFF-4AE5-A1B1-7722ECC6332A}  AccStore Class
{545AE700-50BF-11D1-9FE9-00600832DB4A}  MMCCtrl class
{54702535-2606-11D1-999C-0000F8756A10}  Text Label Class
{548968f5-17f7-4751-a581-ff0f1c732995}  Authentication UI System Settings
{548F0526-B0EC-4915-9C4E-9CEE327CF105}  Browser Setting Handler Factory
{5491AB67-AFEB-48B1-B8DF-B2D63810EF40}  PSFactoryBuffer
{549365d0-ec26-11cf-8310-00aa00b505db}  ADsDSOObject
{549e57e9-b362-49d1-b679-b64d510efe4b}  ShareFlow
{54AF9350-1923-11D3-9CA4-00C04F72C514}  MDACVer.Version
{54B50739-686F-45EB-9DFF-D6A9A0FAA9AF}  PSFactoryBuffer
{54CE37E0-9834-41ae-9896-4DAB69DC022B}  Microsoft RDP Client Control
(redistributable) - version 5a
{54d38bf7-b1ef-4479-9674-1bd6ea465258}  Microsoft RDP Client Control - version 8
{54E211B6-3650-4F75-8334-FA359598E1C5}
{550DDA30-0541-11D2-9CA9-0060B0EC3D39}  XML Data Source Object
{55136805-B2DE-11D1-B9F2-00A0C98BC547}  Shell Name Space
{552E723C-EA6A-499E-9C70-40BC01AEB718}  Explorer Settings Handler(backup only)
{5537E283-B1E7-4EF8-9C6E-7AB0AFE5056D}  CRasProvider
{553858A7-4922-4e7e-B1C1-97140C1C16EF}  IE Component Categories cache daemon
{555278E2-05DB-11D1-883A-3C8B00C10000}  Scale
{555F3418-D99E-4E51-800A-6E89CFD8B1D7}  HWDeviceCustomProperties
{556937b4-9619-4cde-a03b-a0a540bd848c}
Windows.Devices.Bluetooth.Background.BluetoothSignalStrengthTriggerDetails
{5569e7f5-424b-4b93-89ca-79d17924689a}  Windows Media Player Plug-in Registrar
{556FF0D6-A1EE-49E5-9FA4-90AE116AD744}  CLSID_LaunchSettingsPageHandler
{557d33f4-e734-49f4-8b36-0f954d357b1e}  CImeSettingsQuick
{558c258c-90fe-401c-8772-7edca8016d2c}
{558E3D9C-F033-4A44-A019-4F3F39EC8E4F}  DsmUserTask Class
{559C6BAD-1EA8-4963-A087-8A6810F9218B}  CThumbnailGeneratorDmo
{55A371BB-E795-4352-81EE-75721BE523F5}
{55B400DA-2B36-443e-9774-B8C2DAE12FFC}  CLSID_TileBadgeXMLParser
{55b70dec-4b3b-4e26-ae9c-9e8d131843a1}  Microsoft Feeds Background Task Scheduling
{55d7b852-f6d1-42f2-aa75-8728a1b2d264}  Size Categorizer
{5611D887-D47E-4EFC-B390-17F3AEE05B1B}  CLSID_VirtualStream
{56198675-BD59-3B10-8346-583781462CEF}
{562462DD-4F9A-4110-9D6A-C3CA0407FF76}  psfactorybuffer
{56276483-5c2d-472c-b375-23ce4eb6a4f9}  PSFactoryBuffer
{5635493f-7d77-4372-a839-8ad89f5b3726}  Immersive App Context Menu
{563DC062-B09A-11D2-A24D-00104BD35090}  WSHController
{5645C8C1-E277-11CF-8FDA-00AA00A14F93}
{5645C8C2-E277-11CF-8FDA-00AA00A14F93}  MIME Filter
{5645C8C4-E277-11CF-8FDA-00AA00A14F93}
                        Page 58
```

SOFTWARE OUTPUT.txt

```
{565DCEF2-AFC5-11D2-8853-0000F80883E3}
{566A2EFF-5651-4020-AC1A-EB48E4571EA3}  Windows Media SDK HTTP Source Plugin
{5672BB8A-BBF5-482E-B7B9-742C70C604D8}
CAppointmentsProviderInternalShowApointmentDetailsActivationPlugin
{5686a0d9-fe39-409f-9dff-3fdbc849f9f5}  Mpeg4s Decoder MFT
{56871D63-FE46-4c7e-84BB-5DB82D4A99F8}  OOBE Eula Plugin
{56a91da5-5051-49f5-8d23-1f050a63e966}  Use selection check boxes
{56ad4c5d-b908-4f85-8ff1-7940c29b3bcf}  Window Property Store
{56BB05DE-7AFF-49D8-9F54-2D0936D56BF6}
{56DA6136-B95E-4249-BB50-E4773A2B3B5E}  OOBE Proxy Configuration Plugin
{56E0B3FF-1E09-4c99-88B0-C5AAA22E4105}  NarratorTransformPattern Class
{56EA1054-1959-467f-BE3B-A2A787C4B6EA}  SHACCT Profile Notification Handler
{56F62E3E-8904-43F6-B841-DAC177F7FEB9}  Microsoft.WINDOWS.SQLLITE.Params.4.0
{56F68E55-D114-4C64-996E-6E5F2D5340B2}
{56FDF344-FD6D-11d0-958A-006097C9A090}  Task Bar Communication
{57360832-5F9B-4190-8467-000D2D510212}  Language Pack Installer Host
{573bdf38-df23-427f-acb8-a67abd702698}  VssModuleKeeper
{5740A302-EF0B-45ce-BF3B-4470A14A8980}  iTV Capture Feature Segment
{57523D96-B7F6-4D2C-8AFC-BCC5F5392E94}  MSASR Locale Handler Class (1036)
{57558531-C262-471E-95DB-8B181925C61B}  Infrastructure Setup Page Class
{57635537-C856-4cc2-AE5C-62C34708070C}  Shell Security Zone Checker
{57651662-CE3E-11D0-8D77-00C04FC99D61}  CmdFileIcon
{576C5669-E07F-4a1b-9A7A-8F85D944283B}  Search Option Contents Command
{576C9E85-1300-4EF5-BF6B-D00509F4EDCD}  Sync Center Handler Properties Extension
{577289b6-6e75-11df-86f8-18a905160fe0}  Windows Push Notification Platform
Connection Provider
{57756B48-2D36-478F-B4F4-E8C67C5A9454}
{577FAA18-4518-445E-8F70-1473F8CF4BA4}  Utility Object for Binding Events
SubObjects in Script Variables
{57804CEE-0B00-49AC-94FD-F26E474CCE16}  WebCam.ProxyStubFactory
{578fef39-5e60-4aaf-855b-b6be18ac223e}  Family.Authentication.ProxyStub
{5791BC26-CE9C-11D1-97BF-0000F81E849C}  WBEM Scripting Object Path
{579648D9-94B1-418D-ACC6-AFA17860F320}
{5798643F-DC40-47c2-AA81-2D21B96B933E}  PopImapAccountAccessor
{57B67A1A-2C81-4820-96EC-FA33567A9155}  SpTaskManager Class
{57C06EAA-8784-11D0-83D4-00A0C911E5DF}  Microsoft Client Configuration Notify
Object
{57C596D0-9370-40C0-BA0D-AB491B63255D}  IP Security Monitor
{5805137A-E348-4F7C-B3CC-6DB9965A0599}
{581333F6-28DB-41BE-BC7A-FF201F12F3F6}  Radio Management API
{58141F2A-7598-4B93-9D77-4ADF00E044B8}  CLSID_ImmersiveLauncherQueryResultCount
{5815ADD9-95C5-44F2-8262-3BCD56AA3147}  Windows Search Manager Event Sink
{58221C65-EA27-11CF-ADCF-00AA00A80033}  FILEMGMT 1.0 Object
{58221C66-EA27-11CF-ADCF-00AA00A80033}  SvcVwr 1.0 Object
{58221C67-EA27-11CF-ADCF-00AA00A80033}  Computer Management 1.0 Object
{58221C69-EA27-11CF-ADCF-00AA00A80033}  FILEMGMT 1.0 Object
{58221C6A-EA27-11CF-ADCF-00AA00A80033}  SvcVwr 1.0 Object
{5839FCA9-774D-42A1-ACDA-D6A79037F57F}  Microsoft WBEM _WbemFetchRefresherMgr
Proxy Helper
{5842a140-ff9f-4166-8f5c-62f5b7b0c781}  Appx Package API Factory Object
{58476F97-6464-4e49-9BCB-DD88816A60A3}
{5848A73D-E9C2-499E-BB92-887CABCB2BD6}  Microsoft XPS Active Document
{586d1936-bc46-4f9c-bf65-77c95ad9d9ad}  Share Platform Host
{58859c43-2c82-454b-86c0-9efb11e54838}  Ratings Categorizer
{58A9EBF6-5755-4554-A67E-A2467AD1447B}  Setting Content File Persistent Handler
{58AB2366-D597-11d1-B90E-00C04FC9B263}  EapTlsCfg Class
{58C2B4D0-46E7-11D1-89AC-00A0C9054129}  DirectMusicSynth
{58DDEF94-53B5-4BD5-AF79-C4581BBDf7AC}  WISPr Signup Page Class
{58E3C745-D971-4081-9034-86E34B30836A}  Speech Recognition
{58ECEE30-E715-11CF-B0E3-00AA003F000F}  FoxOLEDB 1.0 Object
{58fb76b9-ac85-4e55-ac04-427593b1d060}  Certificate Services Client Task Handler
{59108A76-472B-4311-A9E0-B6FF399B8C99}
{591209c7-767b-42b2-9fba-44ee4615f2c7}  Application Registration
```

Page 59

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {5914e885-9394-4baf-9cd9-71f57e4f6c90} | Family.SyncEngine.ProxyStub |
| {593817A0-7DB3-11CF-A2DE-00AA00B93356} | DirectDraw Clipper Object |
| {593FB605-4854-4965-B5A1-70AB54AB6475} | |
| {594103b8-e428-4461-b8d7-dd0ae12d31d9} | CFileInformationProxy |
| {595397F6-2873-449C-954B-B2E23F89D9D7} | |
| {59549856-D7D2-47DD-ADB7-CEC2E8A7E2C5} | MCCS CardDavSyncEngine |
| {596742A5-1393-4e13-8765-AE1DF71ACAFB} | Microsoft Breadcrumb Bar |
| {59699770-2BF1-46C6-857C-1D509DB7079E} | GlobalServiceDS Class |
| {596AB062-B4D2-4215-9F74-E9109B0A8153} | Previous Versions Property Page |
| {597D4FB0-47FD-4aff-89B9-C6CFAE8CF08E} | ManipulationProcessor Class |
| {59856830-3ECB-4D29-9CFE-DDD0F74B96A2} | |
| {59899957-02f6-44ac-a369-7704e65a1364} | MF MPEG4 Parser Factory |
| {598c2d1b-616c-4782-8cc2-fda9d459be71} | EAPHost Generic Identity UI class |
| {59A437AB-74F3-4de2-AFE6-54203634C4DD} | Share Permission List |
| {59B7DE6C-57AF-11E1-B7A4-EACC4724019B} | SlideShow Setting Handler |
| {59B9640B-3F70-4D1C-B159-F26EEB8A4C87} | Delayed Background Upload Task Handler |
| {59be4990-f85c-11ce-aff7-00aa003ca9f6} | Shell extensions for Microsoft Windows Network objects |
| {59C88A5A-702B-4DAB-9FBE-F53140BA899B} | FhUrlAccessor Class |
| {59CBCF95-7705-43EF-9586-A46B0D03DDE9} | Windows.Management.Workplace.WorkplaceSettings.ProxyStubFactory |
| {59CDB915-8232-46AD-B38B-497B8B0463AD} | Workspace Setup Configure Page |
| {59CE6880-ACF8-11CF-B56E-0080C7C4B68A} | Performance Property Page |
| {59D95679-9799-458F-8B5B-FE00D8DA0AE4} | Microsoft TCPIP WMI Provider |
| {59DC47A8-116C-11D3-9D8E-00C04F72D980} | BDA Tuning Model Component Class(Broadcast Substream) |
| {59F927B8-B249-4672-88D5-2D688BAFDF24} | User Event XML |
| {59FD5FD6-896A-425B-B7B6-E7A0318FC127} | PSFactoryBuffer |
| {5a4b3263-4381-4499-bf2f-c98d168e3ee2} | CImeDictAPIBlockBinder Class |
| {5A57485B-151F-4868-945B-FBB95B574075} | MTF Datasource Manager |
| {5A580C11-E5EB-11d1-A86E-0000F8084F96} | CLSID_IHTTPMailTransport |
| {5a6efd3c-a6b5-44ee-873f-9b25bdbe045b} | Windows.Devices.Background.DeviceUseDetails Factory |
| {5A823D1E-8DDC-44DD-8AB4-F9D32C7FBB05} | IoT Activation Client |
| {5A8A3AAA-D614-46B9-B814-18D168A4B838} | Sync root pause verb |
| {5A8A3AAB-D614-46B9-B814-18D168A4B838} | Sync root unpause verb |
| {5A8A3AAC-D614-46B9-B814-18D168A4B838} | Sync root refresh verb |
| {5A90DD8E-2A0C-45D1-873A-82B61604CEB2} | Setting Content Filter |
| {5AA199A0-1CED-43A5-9B85-3226086738A3} | Binding Engine Task Handler |
| {5AA730D8-0F13-4AD6-B6C6-1EA85218C9A0} | MF MP3 Parser Class Factory |
| {5acb106d-1a06-4fcd-862d-02a74de81835} | Device Property Manager Class |
| {5ADF5BF6-E452-11D1-945A-00C04FB984F9} | WSecEdit Security Configuration Class |
| {5AE1DAE0-1461-11d2-A484-00C04F8EFB69} | Wheel |
| {5AE8571B-DB50-4B7F-9726-64201BED2FC2} | PSFactoryBuffer |
| {5AFFD66E-3C01-4217-BE18-414C155F67B1} | Authentication UI Shutdown Flyout |
| {5B035261-40F9-11D1-AAEC-00805FC1270E} | Network Configuration Component Object |
| {5B18AB61-091D-11D1-97DF-00C04FB9618A} | Microsoft DTC Transaction Manager |
| {5b389765-edc1-4adf-9812-1c8a83175892} | Pin Property Control |
| {5b4dae26-b807-11d0-9815-00c04fd91972} | Menu Band |
| {5b53b2c2-46d6-433e-ab6e-b82efef22b6e} | ExplorerCommandEnumerator |
| {5B681E0D-BD15-4A0E-8B8C-8E90663344E4} | CertificateStore |
| {5B6D1451-B1E1-4372-90F5-88E541B4DAB9} | CUpdateEncryptionSettings |
| {5b858418-cfb4-4b32-8501-54d8b0c59f90} | Item Enumerator Over Categories |
| {5B89DEEB-4DF1-4CF6-9979-C79185CB95A0} | ProvOperations |
| {5B9084E3-CE4E-4C66-8713-5B02396C090B} | SpVAEngineModel Class |
| {5b934b42-522b-4c34-bbfe-37a3ef7b9c90} | This Device |
| {5B99FA76-721C-423C-ADAC-56D03C8A8007} | Delivery Optimization Class |
| {5BA7489A-4BBA-4D18-889A-5F725025F268} | |
| {5BE4911E-3D99-4546-898D-7EE70201C519} | Shell User Object |
| {5BF9AA75-D7FF-4aee-AA2C-96810586456D} | |
| {5BFF4E02-D379-4050-A382-C6504A980D46} | PowrProfApi |
| {5BFFA85A-3384-3540-9940-699120D428A8} | OcrEngineStatics |
| {5C03E1B1-EB13-4DF1-8943-2FE8E7D5F309} | MapsIdleBackgroundCopyCallback Class |

Page 60

SOFTWARE OUTPUT.txt

```
{5C0786ED-1847-11D2-ABA2-00C04FB6C6FA}  WSecEdit Security Manager Class
{5C0786EE-1847-11D2-ABA2-00C04FB6C6FA}  WSecEdit Security Settings Class
{5C0D19E4-A364-4ef6-9288-DBD194593879}  Device Center General Property Sheet
{5C140836-43DE-11d3-847D-00C04F79DBC0}  SCPTRANS Class
{5C24B264-3A01-475C-8EE8-ED4B9DC4F86C}  Wireless Setting Monitor
{5c2dc96f-8d51-434b-b33c-379bccae77c3}  AzBizRuleContext Class
{5C5C1935-0235-4434-80BC-251BC1EC39C6}
{5C63C1AD-3956-4FF8-8486-40034758315B}  Home Networking Sharing Configuration
Manager
{5C659257-E236-11D2-8899-00104B2AFB46}  WMISnapin Class
{5C659258-E236-11D2-8899-00104B2AFB46}  Allows configuration and control of the
Windows Management Instrumentation (WMI) service.
{5c70bc6a-4ab5-48ee-bce3-e6dd857cbdc6}  Sort Ascending Explorer Command
{5C917E9C-0B2F-40D6-928B-5C43FDB16DF4}  Developer License Launcher
{5C9EA9AA-5541-49C5-97C4-781B1E720F5C}  Tablet Mode Controller
{5CAF7D9E-6DDC-409F-8C87-065FC3B194E6}  TextRendererInproc Class
{5cb0d309-91e1-4d75-82f6-6536909c1286}  CloudExperienceHost.ProxyStub
{5cb66670-d3d4-11cf-acab-00a024a55aef}  COM+ Extended Transaction Context
Component
{5cd80a0d-5627-49ff-ad53-c8b1791c85f6}  TTLS Identity UI class
{5CE34C0D-0DC9-4C1F-897C-DAA1B78CEE7C}  PSFactoryBuffer
{5D02926A-212E-11D0-9DF9-00A0C922E6EC}  Microsoft InfoTech IStorage System
{5D084DCB-C187-4bdc-95D1-929CC8418BF8}  Package Information
{5D08B586-343A-11D0-AD46-00C04FD8FDFF}  Microsoft WBEM Event Subsystem
{5d1026ee-3f2e-4ccb-a83d-cefb7ac22a71}  Share Media Control Panel
{5D2F9804-2614-47e5-9B39-C9F74F51FE98}  NarratorSpinner Class
{5D429AF6-D20F-4363-B378-C4AA2FA685EE}  OOBE HidKeyboardPairing Wizard Page
{5D43F9BA-EE77-485B-ACFC-4AD067DAF7BD}  IME JPN Setting Handler
{5d4d54b3-9fb4-4662-8173-c48568d5e79e}  Percent Categorizer
{5D6179C8-17EC-11D1-9AA9-00C04FD8FE93}  Microsoft Local Users and Groups MMC
Snap-in
{5D6179D2-17EC-11D1-9AA9-00C04FD8FE93}  Microsoft Local Users and Groups MMC
Snap-in About Provider
{5d7222bc-b407-410b-b440-080f8172ca09}  PSFactoryBuffer
{5D75245F-29AE-450D-8924-A7611DE279AF}  Drive Defragment Command
{5d8d315e-8adc-48e5-80ed-7ccf370c971f}  EAP MSCHAPv2 Identity UI class
{5D8E73F7-4989-4ac8-8A98-39BA0D325302}  MSVidCtl Digital TV to iTV Composition
Segment
{5D9DD151-65F4-11CE-900D-00AA00445589}  Microsoft DTC Transaction Manager Proxy
(private, internal)
{5DA8B048-EEB0-4c15-9BB9-F2CF953C4F47}  NarratorCheckBox Class
{5da8fe1f-f485-4516-be06-426b0dddf555}  ShellBrowserWindow Class Factory
{5DB2625A-54DF-11D0-B6C4-0800091AA605}  ICM Monitor Management
{5DC41690-C6A6-11d1-9D35-006008B0E5CA}
{5DC41691-C6A6-11d1-9D35-006008B0E5CA}
{5DC41692-C6A6-11d1-9D35-006008B0E5CA}
{5DC41693-C6A6-11d1-9D35-006008B0E5CA}
{5DC41694-C6A6-11d1-9D35-006008B0E5CA}
{5DE7918B-BFD7-4C1E-B4E0-B16D0A3EA76B}  PSFactoryBuffer
{5E032150-8C1E-4c9e-BC60-36E9BFFCFF56}  HomeGroup Peer Manager
{5E1395B2-B685-44e3-8AED-E2304D85ACD1}  WiaWow64
{5E33D52F-2EE2-48EE-80FC-543DFF43E326}  IGD Helper Class
{5E5F29CE-E0A8-49D3-AF32-7A7BDC173478}  This PC
{5E6AB780-7743-11CF-A12B-00AA004AE837}  Microsoft Internet Toolbar
{5e941d80-bf96-11cd-b579-08002b30bfeb}  Plain Text persistent handler
{5ead82c2-28f1-4f7f-956d-d37420b5a687}  Mobile Broadband Connecting Page Class
{5ED4F38C-D3FF-4D61-B506-6820320AEBFE}  PC Settings
{5ef4af3a-f726-11d0-b8a2-00c04fc309a4}  Recycle Bin Cleaner
{5F02227D-BF38-48BE-B01A-A47D3006DFA2}  WPDDispatchFactory Class
{5F293F05-14BA-40b9-AE65-58B034579917}  NarratorIPAddress Class
{5F35421F-3313-4AD6-A3D9-DC4CD7DB4BED}  PSFactoryBuffer
{5f4baad0-4d59-4fcd-b213-783ce7a92f22}  WIA Event Prompt Class
{5F5295E0-429F-1069-A2E2-08002B30309D}  Drive Property Page Extension
```

Page 61

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {5F5AFF4A-2F7F-4279-88C2-CD88EB39D144} | Microsoft MPEG-2 Encoder |
| {5F681803-2900-4C43-A1CC-CF405404A676} | Microsoft RDP Client Control |
| (redistributable) - version 9 | |
| {5f6c1ba8-5330-422e-a368-572b244d3f87} | PSFactoryBuffer |
| {5f7f3f7b-1177-4d4b-b1db-bc6f671b8f25} | User OOBE Create User Object Server |
| {5F884992-EE6D-418B-9E6C-0C2A0FA94D17} | Device Center Hardware Property Sheet |
| {5FA29220-36A1-40f9-89C6-F4B384B7642E} | Shell Message Handler |
| {5FB6752A-59BD-4385-8753-13DEFB1AE728} | NarratorTab Class |
| {5FB7EF7D-DFF4-468a-B6B7-2FCBD188F994} | SpMemoryStream Class |
| {5FDD51E2-A9D0-44CE-8C8D-162BA0C591A0} | |
| {6004c347-d3f3-472a-8f9e-319b5c583d55} | DESC_ItemThumbnail |
| {600e7adb-da3e-41a4-9225-3c0399e88c0c} | CngCredUICredentialProvider |
| {600f8139-d614-4700-bf13-b0ccf9818c73} | |
| {60134A79-1A65-41b5-AC93-8443DB17D3A2} | LockScreen Notification Parser |
| {60173D16-A550-47f0-A14B-C6F9E4DA0831} | Mount Point Rename |
| {60254CA5-953B-11CF-8C96-00AA00B8708C} | Shell Extension For Windows Script Host |
| {602BDCE5-CA64-4E91-B27C-FFCA48978A00} | Windows Search Index Notification Sink |
| {6038EF75-ABFC-4e59-AB6F-12D397F6568D} | IE Microsoft History AutoComplete List |
| {603D3800-BD81-11d0-A3A5-00C04FD706EC} | Background Task Scheduler |
| {603D3801-BD81-11d0-A3A5-00C04FD706EC} | Shared Task Scheduler |
| {60400283-b242-4fa8-8c25-caf695b88209} | Device Installation Group Policy Task |
| Handler | |
| {6047F837-D527-467E-9DC1-6D51F92D9E45} | Wordpad ODT Filter |
| {60632754-c523-4b62-b45c-4172da012619} | User Accounts |
| {60664caf-af0d-0005-a300-5c7d25ff22a0} | Shell Local Machine Object |
| {606B3777-3051-401F-974A-E66ACA82A3A3} | Superseded Updates Cleanup |
| {607fd4e8-0a03-11d1-ab1d-00c04fc9b304} | CoICOFilter Class |
| {6089A37E-EB8A-482D-BD6F-F9F46904D16D} | AccServerDocMgr Class |
| {60912A1F-A6E6-4C7F-8E2D-8BE7C6505E2D} | MicrosoftAccountExtensionFactory |
| {60A4C78C-E2B8-4E6E-876F-DA203B02C05E} | Backup Upload Task Handler |
| {60ABC2F2-6305-4E03-8645-5F9BA071954B} | OOBE UpgradeApps Plugin |
| {60b78e88-ead8-445c-9cfd-0b87f74ea6cd} | PasswordProvider |
| {60EA900E-0F60-4246-8B09-4E890711701D} | ImeBrokerClient_CHT Class |
| {60F6E464-4DEF-11d2-B2D9-00C04F8EEC8C} | Old Files In Root Prop Bag |
| {60F6E465-4DEF-11d2-B2D9-00C04F8EEC8C} | Temp Files Prop Bag |
| {60F6E466-4DEF-11d2-B2D9-00C04F8EEC8C} | Setup Files Prop Bag |
| {60F6E467-4DEF-11d2-B2D9-00C04F8EEC8C} | Uninstall Prop Bag |
| {60F9F51E-4613-4b35-AE88-332542B567B8} | MF Fragmented MPEG4 Sink Class Factory |
| {60fd46de-f830-4894-a628-6fa81bc0190d} | DropTarget Object for Photo Printing |
| Wizard | |
| {6129C4B2-9397-4E58-BCD8-CED219D0CD33} | LocationRevocationHandler |
| {6131A8EC-78CE-11d2-A3F2-3078302C2030} | |
| {613fba38-a3df-4ab8-9674-5604984a299a} | |
| {614C2902-8C8F-4D8F-90A2-FB9017B19FF9} | FhTargetMigration Class |
| {61625667-893E-4707-B925-A82B528C00B8} | APVisual |
| {61667EE4-8071-46E2-9016-3DB2D7BE9E28} | Connected Account Services |
| {6173D628-67F9-49B5-B9C1-D7ABD9E70D34} | Network Category |
| {61b68808-8eee-4fd1-acb8-3d804c8db056} | Contact class |
| {61B7F4E6-ECD0-4da8-AB2F-9517CDB4B8F1} | ChsWubiDS |
| {61E79517-4A4E-45D8-9219-30E71A9EFF39} | TabletButtonExtendedActions Class |
| {61f77d5e-afe9-400b-a5e6-e9e80fc8e601} | RetailDemo Cleanup offline content Task |
| Handler | |
| {61F7B364-432C-4D04-BBC1-7FC1BF3807A8} | Bluetooth Bluewire Shell property |
| extension object | |
| {62079164-233b-41f8-a80f-f01705f514a8} | EVR Graph Optimizer |
| {6208889B-F7A7-44B4-A34E-3C40E83281DB} | OOBE LocalUser Wizard Page |
| {62112AA1-EBE4-11cf-A5FB-0020AFE7292D} | Shell Automation Folder View |
| {6223D62D-9248-4f6b-88AE-336E54ECC887} | Start Layout Setting Monitor |
| {622A8646-1096-4765-8E07-91A3E661CEF9} | HomeGroup Task |
| {62323107-AD7E-49D1-9223-7ADD7C922D1B} | RASGCW Control Class |
| {623E2882-FC0E-11d1-9A77-0000F8756A10} | Gradient |
| {62547D24-2ACA-4A33-8F15-AE95CE1A45BD} | SpFileStream Class |
| {626BAFE6-E5D6-11D1-B1DD-006097D503D9} | CLSID_OERulesManager |

Page 62

SOFTWARE OUTPUT.txt

```
{626C80C1-D410-4DE4-9E82-1B4B9610C404}   SpSharedAudioIn Class
{6279b7cb-d768-4fbe-a6d5-add4f711e53b}   Microsoft IME SingleKanjiDictionary
interface
{6295DF27-35EE-11D1-8707-00C04FD93327}   Sync Manager (Legacy)
{6295DF2D-35EE-11D1-8707-00C04FD93327}   Sync Center (Private)
{62AAAC25-625B-4297-9842-8E4442FA98F5}   DIALServerControl Factory
{62ADD3C3-2648-41E3-A142-5F379BE9229A}   IP Receiver Data Plugin
{62AE1F9A-126A-11D0-A14B-0800361B1103}
{62BE5D10-60EB-11d0-BD3B-00A0C911CE86}   System Device Enumerator
{62CE7E72-4C71-4D20-B15D-452831A87D9D}   Microsoft H264 Video Decoder MFT
{62D8ED13-C9D0-4CE8-A914-47DD628FB1B0}   Region and Language
{62E607F5-D6C2-4F5C-92EF-0D68452F5715}   Package State Handler Factory
{630BB917-AA3B-4CF5-9D24-AAD1F7D4297A}   SmRecipientCollection
{6311429E-2F1A-4777-880F-C7289FD10169}   Inplace Share Engine
{6312362E-EDA0-42BA-B7B1-9C8FE3D4D1A4}   SmEntryId
{631E88E6-45C5-40DC-B2D4-28B732E45F96}   PlayToReceiver Manager
{63260bce-a3fb-4a34-aa51-d4d8e877b62b}   Work Folder Maintenance Task Class
{6329947b-0b98-4bce-91e1-f90e7a84cd16}   AppServiceServiceComponent
{632A2D3D-86AF-411A-8654-7511B51B3D5F}   Lattice Class
{632B0530-3CBF-44F4-BFDC-750A80D4B00A}   StateController Class
{6348A566-0BB9-425C-8E5A-F7ECDCD0419B}   Wallet.WalletBackgroundServiceProxyFactory
{634F8410-E924-46B8-A1B5-E8B08E8B8750}   PSFactoryBuffer
{636B1538-4AD1-4FA5-831A-403D7146B11D}   SpITNProcessor Class
{636B9F10-0C7D-11D1-95B2-0020AFDC7421}   DirectMusic
{636c15cf-df63-4790-866a-117163d10a46}   MFRemoteDesktopPlugin Class
{6377013E-2C35-40F3-B8E1-1AB47D12982B}   WABSyncProvider
{638DA67A-FAF8-4148-8DAE-9AB433DE470D}   NarratorGridPattern Class
{639bdb5a-7959-48d4-afc3-44f252bf2924}   Cached File Updater Placeholder Stream
Resolver
{639F5AF5-BCED-4369-AC34-360B16D955FD}   GestureRecognizer Class
{63A4B1FC-259A-4A5B-8129-A83B8C9E6F4F}   Strips
{63B51F81-C868-11D0-999C-00C04FD655E1}   Shell Icon Overlay Manager
{63da6ec0-2e98-11cf-8d82-444553540000}   Microsoft FTP Folder
{63df056d-a8c7-4a2e-87ff-215de332c21f}   MF SVR Proxy/Stub
{63FA5E69-87FE-432d-8F62-9D7A3D7D09C3}   WMPlayer VideoPerfPropPage Class
{641ABA69-56FD-4029-A445-4D8375D3A699}   UIAnimationDiagnostic
{64226369-CCEB-477D-88D5-7A9CB465BEAC}   Identity Web Wizard Control
{6438570B-0C08-4A25-9504-8012BB4D50CF}   Tuner Marshaling Helper
{6447ABFE-B1CF-4F4D-BE2D-4924C8C8FE00}   SelectionChangedEvent Class
{6447E897-294B-409A-BF15-5F349A20F2C0}   OOBE Registered Owner
{64577982-86D7-11d1-BDFC-00C04FA31009}   CLSID_IHashTable
{6468e186-485e-47e4-83d8-8d9318675219}   Logon Status String Helper
{64693913-1c21-4f30-a98f-4e52906d3b56}   CLSID_AppInstanceFolder
{6473E7E7-D8D6-4696-9FBB-9F41DF134B7B}   Invitation Record XML
{649b3cc6-4621-413f-a08b-5aedd333ff6b}   CMCSFFactory
{649c5690-507e-494a-9e89-1eb24e4bce3d}   WMPMDE LPCM SINK ACTIVATE
{649EEC1E-B579-4E8C-BB3B-4997F8426536}   DXTFilterBehavior
{64AB4BB7-111E-11d1-8F79-00C04FC2FBE1}   Microsoft Shell UI Helper
{64B8F404-A4AE-11D1-B7B6-00C04FB926AF}   PSFactoryBuffer
{64BC32B5-4EEC-4de7-972D-BD8BD0324537}   Search Control
{64D8A8E0-80A2-11d2-8CF3-00A0C9441E20}   RenderEngine Class
{64EE4BAC-1027-4736-904D-8BE23B93F82C}   NarratorHyperLink Class
{64FE8D29-91B5-42C4-A7CA-BC2DE782205A}   SyncProxy
{6504AFED-A629-455C-A7F1-04964DEA5CC4}   BDA Tuning Model ISDB Satellite Locator
{6515834D-6125-4878-A3A3-6B0A73B809A2}   Win32_JobObjectLimitInfo Component
{6522CF99-94C7-4958-B18D-4F6159E6926B}   Policy for DWM items tree item callback
object for sysdm.cpl
{652527C4-4A72-4bd3-BFAB-4B06AB172D7C}   Save Search Command
{65303443-AD66-11D1-9D65-00C04FC30DF6}   OleCvt Class
{6543D242-A80B-44A3-B828-95C1EC452423}   ActualWbemAuthenticatedLocator Class
{655D9BF9-3876-43D0-B6E8-C83C1224154C}   SpAudioOrchestratorPolicy Class
{65704743-2513-4987-9fc9-826bbedde743}   UserDeviceRegistration
{6572EE16-5FE5-4331-BB6D-76A49C56E423}   AccDictionary Class
```

Page 63

SOFTWARE OUTPUT.txt

```
{65964407-a5d8-4060-85b0-1ccd63f768e2}  WTV Bytestream Plugin
{659cdea7-489e-11d9-a9cd-000d56965251}  Background Intelligent Transfer Control
Class 3.0
{659CDEAD-489E-11D9-A9CD-000D56965251}  PSFactoryBuffer
{659CDEAE-489E-11D9-A9CD-000D56965251}  psfactorybuffer
{65BD0711-24D2-4FF7-9324-ED2E5D3ABAFA}  MediaDet
{65CD43A2-C66C-4C0C-9EC6-6F3D619E67AB}  CLSID_MIMEEntity
{65d00646-cde3-4a88-9163-6769f0f1a97d}  InkOverlay Class
{65d4221e-35c4-4a66-bdfa-f080bec22720}  Windows.Internal.Bluetooth Proxy
{65EE1DBA-8FF4-4a58-AC1C-3470EE2F376A}  VSSoftwareProvider Class
{660b90c8-73a9-4b58-8cae-355b7f55341b}  Start Menu Cache
{66182EC4-AFD1-11d2-9CB9-0000F87A369E}  WinNT System Info Object
{661FF7F6-F4D1-4593-B59D-4C54C1ECE68B}  WmiPerf Class Provider
{66275315-bfa5-451b-88b6-e56ebc8d9b58}  Library Property Handler
{66742402-F9B9-11D1-A202-0000F81FEDEE}
{667955AD-6B3B-43CA-B949-BC69B5BAFF7F}  DirectPlay8LobbiedApplication Object
{66a1c746-b147-43b8-8d08-a2657bebbe8f}  OOBE User Manager
{66B8AA0A-7AA7-4BE6-8F37-344D5767240F}  dialclient
{66c2c36e-a363-434c-8e61-e488f0b116f7}
{66D0DB14-5638-475f-A386-629522D8C461}  ConfigManager2
{66d56b60-97b7-4e6a-9aa1-3ec5e3fdaa0f}  Winsock Diagnostic Helper Class
{66e4e4fb-f385-4dd0-8d74-a2efd1bc6178}  Shell Image Data Factory
{66EC5C50-45B7-48cd-81D6-20A712011AD1}  SpeechUXHost Class
{66eea0f5-001a-4073-a496-783f86fcf4c0}  Windows Data Burn
{6705C562-0AE7-40EA-8474-F39DAB1813D0}  RAS Media Manager
{671FCFDA-4BE4-432c-A6D3-4179179C3856}  NarratorSelectionItemPattern Class
{6746c347-576b-4f73-9012-cdfeea251bc4}  CLSID_ScopeFactory
{674B6698-EE92-11D0-AD71-00C04FD8FDFF}  Microsoft WBEM Call Context
{6756A641-DE71-11d0-831B-00AA005B4383}  MRU AutoComplete List
{675F097E-4C4D-11D0-B6C1-0800091AA605}  ICM Printer Management
{67677441-3350-45B4-9455-4D7F4A50F4E4}  SpLexicon Class
{67718415-c450-4f3c-bf8a-b487642dc39b}  Windows Features
{677561f9-50fc-4b24-921d-eacb89706059}  AirplaneModeAPI
{6785BFAC-9D2D-4be5-B7E2-59937E8FB80A}  Other Users Folder
Fri Jul 10 11:05:03 2015 Z
{67A66362-050E-42ff-B241-82C1F51EA9B9}  State and invocation of verb commands
exposed by CommandFolder
{67CA7650-96E6-4FDD-BB43-A8E774F73A57}  HomeGroup Control Panel
{67EA3D48-83F2-408C-AD46-97F207D79DB3}  SpDMOAudioIn Class
{67F07E00-CCEF-11D2-9EF9-006008039E37}  Audio Mixer Property
{681FD532-7EC2-4548-9ECE-44AABCFBD254}  Registry Provider Class
{682159d9-c321-47ca-b3f1-30e36b2ec8b9}  CLSID_DesktopExplorerHost
{6833568B-541D-4290-AF22-3AFB73D1447C}
{683a732e-eee1-4aec-8b45-455890e87ff1}  Retrying APN Class
{687529e6-4d36-4336-88ea-94b03d16aa4b  Device Pairing Container
{687607A0-6BA1-4355-99F4-4E3D749FFB19}  WlanDlgOneXUIPage Class
{687D3367-3644-467a-ADFE-6CD7A85C4A2C}  MPEG-2 Demultiplexer(NoClock)
{687e55ca-6621-4c41-b9f1-c0eddc94bb05}  SdController Class
{68904ac7-1801-47f8-af3a-dac14848fd75}  PSFactoryBuffer
{68b07bff-cb50-4d60-a7d5-02b1a523bc8c}  SearchConnector Icon Extract Extension
{68B67DA9-7212-396E-9528-33F70547660E}
{68c67565-410e-45e6-8560-4091ae193481}
{68cfb337-fd99-43af-a64f-8b84c9ce6a56}
{68DB2410-63D2-4D4A-9449-FBD53FA4E7A3}  OOBE LocalUser Plugin
{68ddbb56-9d1d-4fd9-89c5-c0da2a625392}  UnexpectedShutdownReason
{68E3F2FD-31AE-4441-BB6A-FD7047525F90}
{68e52c1c-37cb-41d2-afe1-1e77d5f10676}  Autoplay Device Event Handler Info
{69127644-2511-4DF5-BC6A-26178254AA40}  RemoteAssistance Class
{692A9F02-84DE-468b-A549-B30AEC43FFF2}  CLSID_AppSpaceImage
{6935DB93-21E8-4ccc-BEB9-9FE3C77A297A}  Custom MRU AutoCompleted List
{693644B0-6858-11D2-9EEB-006008039E37}  Still Video Property Page
{69546697-5b53-43c5-8391-9e227b54957b}  IARPUninstallerProxy
{698A4FFC-63A3-4E70-8F00-376AD29363FB}  Wordpad OOXML Document Filter
```

Page 64

SOFTWARE OUTPUT.txt

```
{699583D1-6BA0-4DF2-B559-2487ED3A58CB}  Device metadata helper
{699745C2-5066-4B82-A8E3-D40478DBEC8C}
{69A0BC0E-7B4E-4EE4-83B5-6C5CE096DAAE}  ImeSystrayMenu Class
{69A25C12-1811-11D2-A52B-0000F803A951}
{69A25C14-1811-11D2-A52B-0000F803A951}
{69a568cf-86d1-4e47-b1fc-a74a110583fb}  Manage Library verb
{69A95A38-C637-46A0-9FB2-1C939AEBF2E8}  psfactorybuffer
{69AD4AEE-51BE-439b-A92C-86AE490E8B30}  Legacy Background Intelligent Transfer
Control Class
{69B1A7D7-C09E-40e9-A1DF-688007A2D9E4}
{69B37063-2BB6-43b5-A109-60E69A77840F}  WcsPlugInService Class
{69BE8BB4-D66D-47C8-865A-ED1589433782}
{69C725BB-1A00-496F-A9D6-92F94AFB3DE8}  Window Colorization Settings
{69F14E67-6183-4854-A16C-74273814F10C}  Windows.Devices.SerialCommunication
{69F31C37-09E1-433b-AECB-EBC83E4065D9}  File Change Tracker
{69F9CB25-25E2-4BE1-AB8F-07AA7CB535E8}  Sync Center Isolation Collection (Private)
{6A01FDA0-30DF-11d0-B724-00AA006C1A01}  CoSniffStream Class
{6A08CF80-0E18-11CF-A24D-0020AFD79767}  ACM Wrapper
{6A205B57-2567-4a2c-B881-F787FAB579A3}  Microsoft DocProp Inplace Calendar Control
{6A206B40-465E-487A-AD5C-CCE637EA9EDA}
{6A2A9381-5A92-4296-9397-564673AE1FDD}  CLSID_HomeGroupListenerNotify
{6a2af23e-b6d9-4a72-938d-9bffc96be71e}
Windows.Networking.HostName.ProxyStubFactory
{6A323D92-38A8-449B-8A98-CB1CF3903F5B}  Print Platform PrintSchema
{6a498709-e00b-4c45-a018-8f9e4081ae40}  CImeServerChs
{6A49950E-CE8A-4EF7-88B4-9D112366511C}  SoftKbdRegistry Class
{6A514DB9-3EC1-4F36-9F95-BC0B00152D0B}  DefinitionParser Class
{6A5B0C7C-5CCB-4F10-A043-B8DE007E1952}  MsRdpClientShell Class
{6A5FEA5B-BF8F-4EE5-B8C3-44D8A0D7331C}  PSFactoryBuffer
{6A68CC80-4337-4dbc-BD27-FBFB1053820B}  CSearchLanguageSupport Class
{6A6F4B83-45C5-4ca9-BDD9-0D81C12295E4}  Microsoft RDP Client Control
(redistributable) - version 4a
{6a91029e-aa49-471b-aee7-7d332785660d}  Microsoft IME (Japanese)
{6aa17c06-0c75-4006-81a9-57927e77ae87}  Change Library Icon verb
{6ACB028E-48C0-4A44-964C-E14567C578BA}  SppWmiProvider
{6AD28EE1-5002-4E71-AAF7-BD077907B1A4}  MSVidCtl MPEG2 Decoder to Closed
Captioning Composition Segment
{6AD7D671-3199-4D10-9372-F44DAF1DC867}
{6AE29350-321B-42be-BBE5-12FB5270C0DE}  Microsoft RDP Client Control - version 5
{6af6b181-3a90-4fac-9655-b34041d46b8f}  PSFactoryBuffer
{6AFCCE9E-85F0-475C-944E-9357B84A4975}  Infrastructure Error Page Class
{6AFE625A-6ED7-4475-BD04-47170B77D584}  Setting Unit Factory
{6B0182CC-5D01-4AA2-B295-B99C1451ECA0}  WebProviderTokenResponse Object
{6B0B3E6B-A2C5-4514-8055-AFE8A95242D9}  Microsoft FLAC Audio Decoder MFT
{6B127DF8-E5D6-42CA-B6A8-2FDA5F7FAB17}  WebTokenResponse Object
{6B13B293-30FD-4abb-8E41-29B1F88297E2}  Windows Media Player OCXGeneralPropPage
Class
{6b19c2a9-50ba-4275-b99b-13dcf69b9f19}  NFC Radio Media Manager
{6B273FC5-61FD-4918-95A2-C3B5E9D7F581}
{6B2D6BA0-9F3E-4f27-920B-313CC426A39E}  Open Packaging API Factory Object
{6b33163c-76a5-4b6c-bf21-45de9cd503a1}  Shell Publishing Wizard Object
{6B34D24A-213B-4929-A8A1-F0A94EBDC8BF}
{6b3598cc-db4d-4992-95b9-5d7d327c0dc7}  Validate Server Cert UI class
{6B362280-6915-11D2-951F-0060081840BC}  Silence Generator Property Page
{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}  ShellServiceHost
{6B462062-7CBF-400D-9FDB-813DD10F2778}
{6B4ECC4F-16D1-4474-94AB-5A763F2A54AE}  IE Tracking Shell Menu
{6B6F9D2D-6D49-4026-83A6-86DFC1C3C6F0}  INI Property Set Storage Handler
{6B7F33AC-D91D-4563-BF36-0ACCB24E66FB}  MsRdpSessionManagerSingleUse Class
{6B8195EE-950E-4F71-86F3-ADD77B191420}  Min SI Host Extension Share Platform Host
{6B831E4F-A50D-45FC-842F-16CE27595359}  Storage Processor Default Confirmation UI
{6BA8349F-FDF4-4246-A724-32C943AED24F}  ApplicationTriggerPolicy
{6BC09692-0CE6-11D1-BAAE-00C04FC2E20D}  IAS Attribute Dictionary
```

Page 65

SOFTWARE OUTPUT.txt

```
{6BC0969D-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0969F-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096A0-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B3-0CE6-11D1-BAAE-00C04FC2E20D}    IAS Pipeline
{6BC096B7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096BC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096C6-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096C8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096D5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DA-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DB-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DE-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DF-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E0-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09894-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09896-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09897-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09898-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09899-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989A-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989B-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989C-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989D-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989E-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989F-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A4-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A6-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A9-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC1CFFA-8FC1-4261-AC22-CFB4CC38DB50}    Default Video Renderer
{6BC752F7-9721-49F8-873B-9FECB6215DE3}    Sync Status Property Handler
{6bdadf65-eb94-419b-907c-0ba9dda7f0df}    CImeRequestSender_JK Class
{6BF0A714-3C18-430b-8B5D-83B1C234D3DB}    PSFactoryBuffer
{6BF52A52-394A-11d3-B153-00C04F79FAA6}    Windows Media Player
{6BFCACDC-A6A6-4343-9CF6-83A83727367B}    SpSwVAEngine Class
{6c19be35-7500-11d1-ad94-00c04fd8fdff}    Microsoft WBEM Event filter marshaling
proxy
{6C337B26-3E38-4F98-813B-FBA18BAB64F5}    Reader Search Handler
{6C3EE638-B588-4D7D-B30A-E7E36759305D}    Activation Manager Shim FTM
{6C5CFCDA-1F1A-4c9e-8D65-94771169D0B9}    GameDetails Class
{6C752774-29FB-4e50-8BB1-97098425A77C}    MetadataPackageSource Class
{6C842E43-3809-4E31-9A68-FA587A411F47}    WinStore SLS Attribute Provider
{6C8EEC18-8D75-41B2-A177-8831D59D2D50}    Mouse Control Panel
{6c955eca-04ce-4f1e-84fe-d8a526ce3137}    Shell Icon Global Settings
{6ca50344-051a-4ded-9779-a43305165e35}
{6CF9B800-50DB-46B5-9218-EACF07F5E414}    Internet Explorer ETW Collector Service
{6CFAD761-735D-4AA5-8AFC-AF91A7D61EBA}    Mpeg-2 Video Stream Analysis
{6D0F3287-6D07-4234-A3BC-EE1CD693372E}    Video Transcoder
{6D14D8F9-DCB2-427c-91BB-E161E5870FFD}    NarratorElement Class
{6D1841AA-4F32-4FE6-8EF2-09F69CB32F14}    Input Personalization Setting Unit
Resolver
{6d18ad12-bde3-4393-b311-099c346e6df9}    Background Intelligent Transfer Control
Class 2.0
```

Page 66

SOFTWARE OUTPUT.txt

```
{6D3951EB-0B07-4fb8-B703-7C5CEE0DB578}   Advanced Indexing Options Dialog Object
{6D48E7F7-8ECD-404C-8E30-81C49E8E36EE}
Windows.Storage.Search.StorageLibraryContentChangedTriggerDetails Factory
{6D4A3650-628D-11D2-AE0F-006097B01411}   DirectPlay8 Modem Provider Object
{6D5313C0-8C62-11D1-B2CD-006097DF8C11}   Folder Options Property Page Extension
{6D68D1DE-D432-4B0F-923A-091183A9BDA7}
{6D6B3CD8-1278-11D1-9BD4-00C04FB683FA}   Encode Bit String Class
{6D7A4B0E-66D5-4AC3-A7ED-0189E8CF5E77}   WBEM IP Route Event Provider
{6D8BB3D3-9D87-4a91-AB56-4F30CFFEFE9F}   Explorer Search Band
{6d8ff8d2-730d-11d4-bf42-00b0d0118b56}   UPnPEventingManager
{6d8ff8dc-730d-11d4-bf42-00b0d0118b56}   UPnPDynamicContentSource
{6d8ff8dd-730d-11d4-bf42-00b0d0118b56}   UPnPDescriptionManager
{6d8ff8df-730d-11d4-bf42-00b0d0118b56}   UPnPDevicePersistenceManager
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56}   UPnPContainer
{6d8ff8e1-730d-11d4-bf42-00b0d0118b56}   UPnPContainerManager
{6d8ff8e5-730d-11d4-bf42-00b0d0118b56}   UPnPValidationManager
{6d8ff8e7-730d-11d4-bf42-00b0d0118b56}   UPnPContainerManager64
{6d8ff8e8-730d-11d4-bf42-00b0d0118b56}   UPnPContainer64
{6D99EF93-C3AB-4539-8F2D-BB1BEF21D415}   Registry Setting Handler
{6DA736C9-DCDE-4651-82A8-56E4EF1D8DD7}   CLSID_ScfFileExecute
{6DAF9757-2E37-11D2-AEC9-00C04FB68820}   MOF Compiler
{6db29a9b-10d0-4b93-b86a-188fc998eff8}   InfraCreateTask
{6db7cd52-e3b7-4ecc-bb1f-388aeef6bb50}   Windows Push Notification Developer Proxy
Stub
{6DCF75A0-83C9-4175-A7A8-FE3DCF1F94A4}   OOBE RecommendedSettings Plugin
{6DD062C7-B6E6-4702-98B0-6E6AB46C877D}   Security Listener XML
{6DFD7C5C-2451-11d3-A299-00C04F8EF6AF}   Folder Options
{6e18f9c6-a3eb-495a-89b7-956482e19f7a}   WinSAT Accessibility Object
{6e29fabf-9977-42d1-8d0e-ca7e61ad87e6}   UIAutomation Registrar Class
{6e33091c-d2f8-4740-b55e-2e11d1477a2c}   Shell Image Recompression Object
{6E3D2E94-E6D8-4afd-AFDE-ABD26CA88BF5}   FaultrepDataCollectionInProc
{6E449686-C509-11CF-AAFA-00AA00B6015C}   Microsoft Active Setup Engine
{6E4FCB12-510A-4d40-9304-1DA10AE9147C}   InkTablets Class
{6E582707-CCAF-4333-A9B9-3B4F75C362E0}   DeviceOwnershipControl Class
{6E5D1F2A-AF9A-419A-9CAF-C5A5C32C3CF8}   SettingSync GetBackupStatus
{6e682784-1eca-4cf2-988d-96b6e89e9a4d}   CLSID_SearchIDListFactory
{6E78DAD9-E187-4D6E-BA63-760256D6F405}   Microsoft Session And Connection Provider
{6E7E2EF2-F881-472A-8E32-17CA95710402}   MDM Enterprise Application Provider
{6EA4B9B1-0121-46C9-95CF-8E5392CB8234}
Windows.Networking.BackgroundTransfer.ProxyStubFactory
{6EB22881-8A19-11D0-81B6-00A0C9231C29}   Catalog Class
{6EC153C1-371E-47E1-A896-2F7F80EB7842}   psfactorybuffer
{6EDD6D74-C007-4E75-B76A-E5740995E24C}   PSFactoryBuffer
{6EF07F29-F9B8-4DA4-B59E-13DEA060AD60}
{6EFED3B2-34B3-4612-BF6D-2F206C646AAB}   Toast Element Factory
{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}   Microsoft Metadata Policy Layer
{6F26A6CD-967B-47FD-874A-7AED2C9D25A2}   Video Port Manager
{6f33340d-8a01-473a-b75f-ded88c8360ce}   HomeGroup UI Status
{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}   V1PasswordProvider
{6F58F65F-EC0E-4ACA-99FE-FC5A1A25E4BE}   Language Components Installer
{6f5bad87-9d5e-459f-bd03-3957407051ca}   IEWindows
{6F74FDC5-E366-11d1-9A4E-00C04FA309D4}   CLSID_MessageDatabase
{6F74FDC6-E366-11d1-9A4E-00C04FA309D4}   CLSID_FolderDatabase
{6F7C8E8F-DC69-4e3f-BC05-439962A05FD5}   CLSID_HomeGroupProvider
{6F8CF952-B381-44D3-9704-0ED7C3C4E677}   DevicesFlow Class Factory
{6FE54E0E-009F-4E3D-A830-EDFA71E1F306}   Bluetooth Personal Area Connection
{6ffa842b-fd90-4a0e-9315-21c52b2457aa}   CImeKeyMapView_JK Class
{7007ACC1-3202-11D1-AAD2-00805FC1270E}   Dial-up Connection UI Class
{7007ACC3-3202-11D1-AAD2-00805FC1270E}   Inbound Connection UI Class
{7007ACC4-3202-11D1-AAD2-00805FC1270E}   Internet Connection UI Class
{7007ACC5-3202-11D1-AAD2-00805FC1270E}   LAN Connection UI Class
{7007ACC6-3202-11D1-AAD2-00805FC1270E}   VPN Connection UI Class
{7007ACC7-3202-11D1-AAD2-00805FC1270E}   Network Connections
```

Page 67

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {7007ACC8-3202-11D1-AAD2-00805FC1270E} | Network Connections Enum |
| {7007ACD1-3202-11D1-AAD2-00805FC1270E} | Network Common Connections Ui |
| {7007ACD3-3202-11D1-AAD2-00805FC1270E} | Net Connections UI Utilities Class |
| {7007ACD4-3202-11D1-AAD2-00805FC1270E} | PPPoE UI Class |
| {7007ACD5-3202-11D1-AAD2-00805FC1270E} | Shared Access Connection UI Class |
| {7013943A-E2EC-11D2-A086-00C04F8EF9B5} | SpStreamFormatConverter Class |
| {7016F8FA-CCDA-11D2-B35C-00105A1F8177} | Microsoft WBEM (non)Standard Marshaling for IwbemMultiTarget |
| {7022a3b3-d004-4f52-af11-e9e987fee25f} | WPN SRUM COM Server |
| {70351E05-D2BD-4817-9FFD-A6D4A9A90282} | NarratorWindowPattern Class |
| {703574D6-AA1B-4FBF-A938-9A59C89343FA} | Microsoft PCSV Device Provider |
| {7037C8FC-97F7-4AE5-BF2D-5D2660C97878} | Voice Activation Manager Class |
| {703E7517-FA6F-43E2-9418-EFBE2A1357F0} | Windows.ApplicationModel.Wallet.ProxyStub |
| {70438d09-456a-4a6f-86fe-1c1a3afc699e} | Pin To Home Command |
| {7057e952-bd1b-11d1-8919-00c04fc2c836} | Microsoft DocHost User Interface Handler |
| {706A79C0-1AC4-4E25-B311-93B643C1E499} | WinMsoIrmProtector Class |
| {70707B39-B2CA-4015-ABEA-F8447D22D88B} | Microsoft MPEG Audio Decoder MFT |
| {7071EC01-663B-4bc1-A1FA-B97F3B917C55} | Build Connections Options Page Class |
| {7071EC05-663B-4bc1-A1FA-B97F3B917C55} | Display Connection Options Page Class |
| {7071EC07-663B-4bc1-A1FA-B97F3B917C55} | Handle Diagnostics Page Class |
| {7071EC13-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Connect To Internet Page Class |
| {7071EC31-663B-4bc1-A1FA-B97F3B917C55} | ISP Offer Page Class |
| {7071EC32-663B-4bc1-A1FA-B97F3B917C55} | ISP Confirm Page Class |
| {7071EC33-663B-4bc1-A1FA-B97F3B917C55} | ISP CD Page Class |
| {7071EC61-663B-4bc1-A1FA-B97F3B917C55} | Display Internet Existing Connections Page Class |
| {7071EC62-663B-4bc1-A1FA-B97F3B917C55} | Display Work Existing Connections Page Class |
| {7071EC71-663B-4bc1-A1FA-B97F3B917C55} | Create Dial-up Task Class |
| {7071EC75-663B-4bc1-A1FA-B97F3B917C55} | Create VPN Task Class |
| {7071EC77-663B-4BC1-A1FA-B97F3B917C55} | XWizard Factory Generated Class |
| {7071ECA0-663B-4bc1-A1FA-B97F3B917C55} | Connect To Internet Task Class |
| {7071ECA3-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Detection Hook Page Class |
| {7071ECA5-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Creation Hook Page Class |
| {7071ECA7-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Testing Hook Page Class |
| {7071ECA8-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Hook Page Class |
| {7071ECA9-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Diagnostics Hook Page Class |
| {7071ECAF-663B-4bc1-A1FA-B97F3B917C55} | Connect To The Internet Finish Page Class |
| {7071ECB0-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Task Class |
| {7071ECB3-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Detection Hook Page Class |
| {7071ECB4-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Existing Connections Page Class |
| {7071ECB5-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Creation Hook Page Class |
| {7071ECB6-663B-4BC1-A1FA-B97F3B917C55} | XWizard Factory Generated Class |
| {7071ECB7-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Testing Hook Page Class |
| {7071ECB8-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Hook Page Class |
| {7071ECBF-663B-4bc1-A1FA-B97F3B917C55} | Connect To Work Finish Page Class |
| {7071ECE0-663B-4bc1-A1FA-B97F3B917C55} | Connect To Network Task Class |
| {7071ECE5-663B-4bc1-A1FA-B97F3B917C55} | Connect To Network Page Class |
| {7071ECF1-663B-4bc1-A1FA-B97F3B917C55} | Message Page Class |
| {7071ECFA-663B-4bc1-A1FA-B97F3B917C55} | Network Tasks Host Class |
| {70804ECC-7272-4dc8-AFFC-97CD66AAA282} | Windows Desktop Search Map Plugin |
| {7086AD76-44BD-11D0-81ED-00A0C90FC491} | DiskManagement.UITasks |
| {70952C5B-517B-44a1-B9CA-23134DA7D565} | EventQueue Class |
| {709E2729-F883-441e-A877-ED3CEFC975E6} | ProfileNotifyHandler Class |
| {70A92FA3-7FD8-4808-9A05-6B2FD19AA5B3} | Immersive Backstack Manager |
| {70cba7d2-50a5-4383-8aa5-b378c01c7364} | CLSID_LegacyFindFiles |
| {70E102B0-5556-11CE-97C0-00AA0055595A} | Video Renderer |

Page 68

SOFTWARE OUTPUT.txt

```
{70f598e9-f4ab-495a-99e2-a7c4d3d89abf}  WMAudio Encoder DMO
{70f98452-3c38-4271-8e76-6f444852ebc8}  PortableDeviceWiaCompat Class
{70FF37C0-F39A-4B26-AE5E-638EF296D490}  RARegSetting Class
{71285C44-1DC0-11D2-B5FB-00104B703EFD}  Microsoft WBEM (non)Standard Marshaling
for IWbemObjectSink
{713790EE-5EE1-45ba-8070-A1337D2762FA}  WTVFile Thumbnail Handler
{713aacc8-3b71-435c-a3a1-be4e53621ab1}  AnimateWindowSize Object
{71455ADC-0A77-405F-BF67-EA663D276653}  Bluetooth MTP Devices Menu
{7153AC3A-D502-4A96-83AC-32C80FA6844A}  Share Platform Core SIHost Component
{715D9C59-4442-11D2-9605-00C04F8EE628}  SpStream Class
{7165c8ab-af88-42bd-86fd-5310b4285a02}  ContactManager class
{7170F2E0-9BE3-11D0-A009-00AA00B605A4}  TAPI3 Terminal Manager Class
{7173725A-9C0E-44B1-8319-69F7D983E8D6}  Immersive Print Dialog 3D
{717ef4fe-ac8d-11d0-b945-00c04fd8d5b0}  DsPropertyPages.User Special Info
{71932D43-3CA5-46EF-B013-3F9A695996ED}  DMO Wrapper Filter
{719ff33d-43af-4d4a-a89a-1599e6d88a37}  Multiplexing Setting Handler
{71A5EC7F-F325-4376-9D94-622C372E256F}  Srum Proxy Stub
{71C99AB9-508A-4671-8B67-302E098FBFA8}
{71D99464-3B6B-475C-B241-E15883207529}  Sync Results Folder
{71E32BAA-73EE-40a1-933C-F166F0192B72}  Show thumbnails instead of icons tree item
callback object for sysdm.cpl
{71E38F91-7E88-11CF-9EDE-0080C78B7F89}  MTxAS Object
{71f96385-ddd6-48d3-a0c1-ae06e8b055fb}  Explorer Browser
{7210D183-F81E-4CEA-A2B9-E73C4ECB067A}  Windows Search Service WinRT Protocol
Handler
{722b3793-5367-4446-b6bb-db89b05c1f24}  ItemHandlerCache
{72422AA4-3536-41FA-965E-D5D9DD130297}  Per Monitor Desktop Visibility Service
{725BE8F7-668E-4C7B-8F90-46BDB0936430}  Keyboard Control Panel
{725F645B-EAED-4fc5-B1C5-D9AD0ACCBA5E}  File Open Dialog Legacy
{727af81a-cacf-4e37-9df7-a22ed974f298}  Application Data Persistence
{728a21c5-3d9e-48d7-9810-864848f0f404}  Provides access to a portable device using
IPortableDevice
{72967901-68EC-11D0-B729-00AA0062CBB7}  WBEM Registry Property Provider
{72967903-68EC-11D0-B729-00AA0062CBB7}  WBEM PerfMon Property Provider
{72970BEB-81F8-46D4-B220-D743F4E49C95}  Volume Shadow Copy WMI Provider
{72A7994A-3092-4054-B6BE-08FF81AEEFFC}  Sharing Elevated Virtual Factory
{72b36e70-8700-42d6-a7f7-c9ab3323ee51}  Search Connector Folder
{72B624DF-AE11-4948-A65C-351EB0829419}
{72BFEB11-2681-490D-874B-652FC1D75ED8}  UIWrapper Class
{72C24DD5-D70A-438B-8A42-98424B88AFB8}  Windows Script Host Shell Object
{72c57034-02c4-4e9f-bf9c-ca711031757e}  Shell File Operation Undo Unit
{72C984BA-0666-4D3F-A0DE-96BF43838E6E}  Generic Setting Handler Class
{72d3edc2-a4c4-11d0-8533-00c04fd8d503}  ADs Property Entry Object
{72D633FF-401E-4AB4-BF80-143E4E907407}  Applicability Cache Monitor
{72eb61e0-8672-4303-9175-f2e4c68b2e7c}  Namespace Walker
{7312498D-E87A-11d1-81E0-0000F87557DB}  Blur
{73257e95-0378-49d6-a954-44aabc841eab}  Address Acquisition Helper Class
{734AC5AE-68E1-4FB5-B8DA-1D92F7FC6661}  WBEM Ping Provider
{7390f3d8-0439-4c05-91e3-cf5cb290c3d0}  Microsoft RDP Client Control
(redistributable) - version 7
{73959FD1-7360-42F7-807D-622341783DC0}
Windows.Management.Deployment.ProxyStubFactory
{73AD6842-ACE0-45E8-A4DD-8795881A2C2A}  SpInProcRecoContext Class
{73C037E7-E5D9-4954-876A-6DA81D6E5768}
{73CFD649-CD48-4fd8-A272-2070EA56526B}  IE BandProxy
{73D14237-B9DB-4efa-A6DD-84350421FB2F}  MSVidCtl Digital TV to CCA Composition
Segment
{73DA5D04-4347-45D3-A9DC-FAE9DDBE558D}  CSectionList
{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}  Microsoft WMI Provider Subsystem Host
{73FDDC80-AEA9-101A-98A7-00AA00374959}  WordPad Document
{740e40d8-5d9f-46be-98dd-39915e3c32ef}  CLSID_StorageLibraryUI
{740EC24D-46AD-4334-A076-41CCC3F8D9B4}  PBDA Class
{74246bfc-4c96-11d0-abef-0020af6b0b7a}  Device Manager
```

Page 69

SOFTWARE OUTPUT.txt

```
{743a6e3b-a5df-43ed-b615-4256add790b8}  MFPsiFilter
{743B5D60-628D-11D2-AE0F-006097B01411}  DirectPlay8 Serial Provider Object
{743F1DC6-5ABA-429F-8BDF-C54D03253DC2}  DirectPlay8Client Object
{7444C717-39BF-11D1-8CD9-00C04FC29D45}  CryptPKO Class
{7444C719-39BF-11D1-8CD9-00C04FC29D45}  CryptSig Class
{7447A267-0015-42C8-A8F1-FB3B94C68361}
{745057c7-f353-4f2d-a7ee-58434477730e}  AEC
{7455AB0D-4F92-41CE-937A-C47D929EC51E}  Start Menu Layout Setting Handler
{745a5add-6a71-47b9-9bb9-31dd3a6913d4}  Authentication UI CredUI Helper
{74620884-155F-4B72-A4F0-0FADDBC0721E}
```
Windows.ApplicationModel.Appointments.AppointmentStoreNotificationTriggerDetails
Factory
```
{7469AE5E-1CA1-4181-970C-BDFD8EAA2C4F}  PSFactoryBuffer
{7473b52d-97d9-41bb-ae03-2d3d51eb42b8}  CImeFileNameRedirectionManager Class
{74761821-E040-423d-9399-35BBA3ECFFF5}  DA Disconnecting Confirm Page
{7478EF61-8C46-11d1-8D99-00A0C913CAD4}  ComponentData Class
{7478EF65-8C46-11d1-8D99-00A0C913CAD4}  ComponentData Class
{7478EF69-8C46-11d1-8D99-00A0C913CAD4}  PerformanceAbout Class
{74807f67-0058-440d-8600-65541a7fbbea}  PSFactoryBuffer
{7487cd30-f71a-11d0-9ea7-00805f714772}  Background Thumbnail Generator
{749962AB-D849-46D5-A39C-75A8307C2C86}
{74b077e8-32de-40ab-be4e-65609f575459}  Resource Monitor
{74F5A028-DD3C-4724-B0E5-1D8A52C948DD}  Windows Connected Search Web Result
```
Provider
```
{75048700-EF1F-11D0-9888-006097DEACF9}  ActiveDesktop
{750F15AE-EBDB-4B5A-9DBF-CA4F5EC295EA}  Microsoft Power WMI Provider
{7513af53-9c75-4ad4-b47e-8d855099e023}  Safe Save Handle Manager Marshaler
{752438CB-E941-433F-BCB4-8B7D2329F0C8}  FwCpl LUA
{75269C13-41E1-4D0E-B8A0-9F8F22E246C9}  SystemAudioDeviceExclusive Class
{7542E960-79C7-11D1-88F9-0080C7D771BF}  Event Subscription
{7548A939-2776-46CF-8F62-1D1F488DEDF0}  Search Query
{754A73E3-B0A5-4305-A45A-428186716507}  Remote Desktop Services Message Server
```
Class
```
{75510190-5A2A-438E-BDC9-187951198FBF}  SystemMonitorInproc Class
{75587F04-6EFF-443e-BED5-637117299643}  DA Pre-CFE Page
{756c119d-9124-4693-80d8-2c1e49afab1f}  PEAP Interactive UI class
{75718C9A-F029-11D1-A1AC-00C04FB6C223}  WBEM Scripting Sink
{75847177-f077-4171-bd2c-a6bb2164fbd0}  Private Profile Object
{7584c670-2274-4efb-b00b-d6aaba6d3850}  Microsoft RDP Client Control
```
(redistributable) - version 4
```
{75BF9604-626B-4F77-BB6E-8032EAD37D2D}
{75C9378A-7E89-11d2-B116-00805FC73204}
{75dff2b7-6936-4c06-a8bb-676a7b00b24b}  CLSID_SeparateMultipleProcessExplorerHost
{75FC37F9-423B-483F-8A2E-AA2CADA4106F}  PSFactoryBuffer
{7601591E-EEC1-43c9-ACC5-F5EA31C7A364}  WLIDFDProv Class
{760C4B83-E211-11D2-BF3E-00805FBE84A6}  Windows Media Services DRM Storage object
{7658816D-64C1-4483-B831-DDC4470014B2}  NarratorComboBoxEdit Class
{7658F2A2-0A83-11d2-A484-00C04F8EFB69}  CrStretch
{7669CAD6-BDEC-11D1-A6A0-00C04FB9988E}  ProtocolsTable Class
{766BF2AE-D650-11d1-9811-00C04FC31D2E}  HomePage Class
{76765b11-3f95-4af2-ac9d-ea55d8994f1a}  Property System Both Class Factory
{767EE1f6-2006-43EA-8278-90B37AC8FD02}
```
Windows.Security.FileRevocationManagerServer.ProxyStubFactory
```
{76A64158-CB41-11D1-8B02-00600806D9B6}  WBEM Scripting Locator
{76B4FCAC-BB29-11DB-96F1-005056C00008}  PBDA ETFilter
{76be8257-c4c0-4d37-90c0-a23372254d27}  Indexer Status Update Object
{76CCA200-8292-4BC5-B400-9265D00C1193}
{76D0CB12-7604-4048-B83C-1005C7DDC503}
{76DAE2C2-5444-469F-9B1F-A853A5D565E2}  CLSID_LockScreenViewManager
{76f014ec-1b0c-4a15-a029-4c0fdf12b5b1}  Briefcase Storage Object
{76F363F2-7E9F-4ED7-A6A7-EE30351B6628}  Inset
{770e8e77-4916-441c-a9a7-b342d0eebc71}  MF ByteStream Proxy Class Factory
{7724F5B4-9A4A-4a93-AD09-B06F7AB31035}  DirectAccess Media Manager
```
Page 70

SOFTWARE OUTPUT.txt

```
{77324C4A-FFFC-49BA-88D8-E357D83B7DE7}   ContentManagementBroker
{77597368-7B15-11D0-A0C2-080036AF3F03}   PrintUIShellExtension Class
{7760EF40-2920-44BA-8B47-2D42B1740139}   MimeReaderTransportWrapper
{7763B7C0-A5FD-4AA9-BD1B-58B17137236B}   Location Description
{7775dec3-6a3e-4c57-bac2-4f1774e54b1b}   Device Pairing Configuration
{777B6BBD-2FF2-11D3-88FE-00C04F8EF9B5}   SpPhraseBuilder Class
{777BA815-2498-4875-933A-3067DE883070}   XWizard Task Stub
{777BA816-2498-4875-933A-3067DE883070}   XWizard Page Stub
{777BA81A-2498-4875-933A-3067DE883070}   XWizard Virtual Factory
{777BA851-2498-4875-933A-3067DE883070}   XWizard Type plugin for Win32 Class
{777BA853-2498-4875-933A-3067DE883070}   XWizard Type plugin for DUI Class
{777BA87C-2498-4875-933A-3067DE883070}   Public XWizard Manager Class
{777BA8D2-2498-4875-933A-3067DE883070}   Public Simple Marshal Class
{777BA8E3-2498-4875-933A-3067DE883070}   Private XWizard Page Enumeration Manager
Class
{777BA8E5-2498-4875-933A-3067DE883070}   Private XWizard Task Enumeration Manager
Class
{777BA8E7-2498-4875-933A-3067DE883070}   Private XWizard Host Enumeration Manager
Class
{777BA8E9-2498-4875-933A-3067DE883070}   Private XWizard Registry Information
Manager Class
{777BA8F5-2498-4875-933A-3067DE883070}   Private XWizard Registration Manager Class
{777BA8F9-2498-4875-933A-3067DE883070}   Private XWizard Factory Registration
Manager Class
{777BA8FB-2498-4875-933A-3067DE883070}   Private XWizard Type Registration Manager
Class
{777D0CFF-0375-43b9-8532-FB04A4903593}   Windows Media Player Effects Activate
{778DE47F-7ADC-4C4D-974D-771BD1675DC5}   DeviceAccessPolicyManager
{77B6E213-6911-441E-8849-AF63C813D6BE}   Windows.Devices.Lights
{77CA5A70-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Switch Ceremony Page Class
{77CA5A71-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Device Discovery Page Class
{77CA5A72-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire PIN Entry Page Class
{77CA5A73-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire PIN Display Page Class
{77CA5A74-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Push Button Page Class
{77CA5A75-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire PIN Compare Page Class
{77CA5A90-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Failure Page Class
{77CA5AA0-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Classic Task Class
{77CA5AA1-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Discovery Task Class
{77CA5AA2-1D99-4E2A-8D16-D2D7D00E9A9B}   Bluewire Ceremony Task Class
{77F10CF0-3DB5-4966-B520-B7C54FD35ED6}   Custom Destination List
{77F419AA-771A-45ff-AC66-7567FA3243D3}   SMB Share Engine
{77F7F122-20B0-4117-A2FB-059D1FC88256}   WPDServiceProvider Class
{780102B0-C43B-4876-BC7B-5E9BA5C88794}   PSFactoryBuffer
{78065982-b44b-41c6-a9a3-f2fd11746223}   Minimal Share Platform Host
{78103FB7-AED7-4066-8BCD-30BB27B02331}   Microsoft WBEM WMI Object Factory
{781C7DE4-515E-43AD-A394-3768176CAC41}   SwitcherEvent Class
{782FC20A-81CF-43DE-A625-072155BCD30C}   HomeGroup Task
{784215B4-0D2E-11D3-920A-00C0DF10D434}   MediaDetFilter
{7849596a-48ea-486e-8937-a2a3009f31a9}   PostBootReminder object
{784BD832-A28C-409A-B440-DAC2028CFA5E}   ImeTelemetrySingleton
{78530B75-61F9-11D2-8CAD-00A024580902}   MS Timeline
{786CDB70-1628-44A0-853C-5D340A499137}   TabletManager Class
{78788f3f-e820-4d2f-bf5f-3252c7946aa4}   IMEPREDICTPROFILE
{7888E5FE-6C66-4A34-B217-FA2292073F4A}   PSFactoryBuffer
{788B686B-EA20-41CD-A018-1BFD506194B2}   ProtocolForResultsOperation
{78DE489B-7931-4f14-83B4-C56D38AC9FFA}   OneDrive network states cache SSO
{78fe669a-186e-4108-96e9-77b586c1332f}   Content Index Null Stemmer
{7924BBA8-1913-4B0E-8E6F-6F45CE499731}   Microsoft Network Connection Profile WMI
Provider
{793239d0-2bed-4e9a-a276-0c8bf918c42e}   UserDeviceRegistration.Ngc
{79376820-07D0-11CF-A24D-0020AFD79767}   DirectSound Audio Renderer
{7940ACF8-60BA-4213-A7C3-F3B400EE266D}   Setup a Workspace Task Class
{7946ede1-839d-49be-9c1d-27c44529e093}   Minimal Share Flow
```

Page 71

SOFTWARE OUTPUT.txt

```
{794873D1-35DB-44c2-8BD2-F332A433C80E}  FocusMonitor Class
{79512918-11cd-4f7c-a294-de1ff011a194}  DeviceInformationServer
{797A9BB1-9E49-4e63-AFE1-1B45B9DC8162}  DeviceHostICSSupport Class
{797B2BFB-AB33-4850-8126-9A07C20FC628}  Windows.Devices.LowLevel
{798059F0-89CA-4160-B325-AEB48EFE4F9A}  CColorControlDmo
{79834058-0A20-44dc-AD9B-CE07DC6E379C}  DevDetailCSP
{7986d495-ce42-4926-8afc-26dfa299cadb}  Authentication UI Logon UI
{7988B573-EC89-11cf-9C00-00AA00A14F56}  Microsoft Disk Quota UI
{7998DC37-D3FE-487C-A60A-7701FCC70CC6}  Microsoft WBEM A51 Repository
{7999FC25-D3C6-11CF-ACAB-00A024A55AEF}  COM+ Transaction Context Component
{79CEEEBE-BDE0-4C05-9D92-155F78BB7D2B}  Application Activation Client
{79DBA461-677B-448A-8A5E-3006DABAF6F9}  P2P Provider Service
{79DEA627-A08A-43AC-8EF5-6900B9299126}
{79eac9d0-baf9-11ce-8c82-00aa004ba90b}  StdHlink
{79eac9d1-baf9-11ce-8c82-00aa004ba90b}  StdHlinkBrowseContext
{79eac9e0-baf9-11ce-8c82-00aa004ba90b}  URL Moniker
{79eac9e2-baf9-11ce-8c82-00aa004ba90b}  http: Asychronous Pluggable Protocol
Handler
{79eac9e3-baf9-11ce-8c82-00aa004ba90b}  ftp: Asychronous Pluggable Protocol
Handler
{79eac9e5-baf9-11ce-8c82-00aa004ba90b}  https: Asychronous Pluggable Protocol
Handler
{79eac9e6-baf9-11ce-8c82-00aa004ba90b}  mk: Asychronous Pluggable Protocol Handler
{79eac9e7-baf9-11ce-8c82-00aa004ba90b}  file:, local: Asychronous Pluggable
Protocol Handler
{79EAC9F1-BAF9-11ce-8C82-00AA004BA90B}  URLMoniker ProxyStub Factory
{79eac9f2-baf9-11ce-8c82-00aa004ba90b}  Async BindCtx
{79EB1402-0AB8-49C0-9E14-A1AE4BA93058}  PSFactoryBuffer
{79FD7442-008F-42D9-ADFA-377C441D2DB1}  PSFactoryBuffer
{7A076CE1-4B31-452a-A4F1-0304C8738100}  Network and Sharing Center Cpl Elevated
Virtual Factory
{7A0CC021-2939-4379-AA82-12AECC3538F6}  CLSID_INewsgroupHelp
{7A0F6AB7-ED84-46B6-B47E-02AA159A152B}  Simple Conflict Presenter
{7a54bbed-bb9b-425a-8bd7-1a5410923dcf}  CLSID_StartMenuCommandingProvider
{7A56C4CB-D678-4188-85A8-BA2EF68FA10D}  SAMI Byte Stream Handler
{7A63D67D-014E-4f5f-AE9D-CC0C1FE16DAC}  CDomNode
{7A7C3277-8F84-4636-95B2-EBB5507FF77E}  LatLongReport Class
{7A80E4A8-8005-11D2-BCF8-00C04F72C717}  ExtractIcon Class
{7a836eee-3676-46fb-ba6f-2de2ce38cbb3}  NarratorApplication Class
{7a872d34-bc6b-4f83-b199-22e9c0a91ddc}  Credential Provider Framework
{7A9D77BD-5403-11d2-8785-2E0420524153}  User Accounts
{7aa7790d-75d7-484b-98a1-3913d022091d}  Shell FMIFS Wrapper
{7AA809F6-C072-11DF-AC23-18A90531A85A}  FhEngineBackup Class
{7AA809F7-C072-11DF-AC23-18A90531A85A}  FhEngineRestore Class
{7AA809F8-C072-11DF-AC23-18A90531A85A}  FhEngineServicing Class
{7AAE5B4F-488C-419b-95E2-923F2AA70FFD}  Sharing Listener XML
{7AB36653-1796-484B-BDFA-E74F1DB7C1DC}  Microsoft Spell Checker Factory Class
{7AB7DD72-B9BA-4731-94A0-59042760C18B}  OOBE Protection Settings Page
{7abbbcca-e01b-4560-8228-92e1eedbc908}  CLSID_CopyUndoHandler
{7AD84985-87B4-4a16-BE58-8B72A5B390F7}  Play To menu
{7AF4D6DC-F176-4db8-BB59-EB5DAA841844}  TextRenderer Class
{7AFA253E-F823-42f6-A5D9-714BDE467412}  AVI Byte Stream Handler
{7afb974e-3842-4106-a702-82a13e088f46}  CLSID_AppContentPropertyStore
{7B014A0C-A42A-4268-BFE0-AFCA9745CD53}
{7B0C11A0-2FAF-40d4-9FE5-28FA27C85442}  Shallow Search Commmand
{7B19A919-A9D6-49E5-BD45-02C34E4E4CD5}
{7B31547E-EF7E-479b-9494-2216DC179E61}  Autoplay Handler
{7B3BC2A0-AA50-4ae7-BD44-B03649EC87C2}  VPS Decoder
{7b40792d-05ff-44c4-9058-f440c71f17d4}  Windows trace relogging support.
{7b4a83b6-f704-4b77-8e3d-c6087e3a21d2}  Share Command State Handler
{7B5A12E8-0C60-4939-A046-11CF879B19FB}  WlanDlg Get Key Task Class
{7B6EA1D5-03C2-4AE4-B21C-8D0515CC91B7}  Shell Create Object Task Server
{7b81be6a-ce2b-4676-a29e-eb907a5126c5}  Programs and Features
```

Page 72

```
                        SOFTWARE OUTPUT.txt
   {7b8a2d94-0ac9-11d1-896c-00c04Fb6bfc4}  Security Manager
   {7b8a2d95-0ac9-11d1-896c-00c04Fb6bfc4}  URL Zone Manager
   {7B90DAE3-4AD0-4F0D-BE80-A26B296C3156}  HomeGroup Troubleshooter Command
   {7b95d5bd-aac9-4f91-aff2-a2000aa5f42f}  File History Configure AutoPlay Handler
Class
   {7b9e38b0-a97c-11d0-8534-00c04fd8d503}  ADs Property Value Object
   {7BA4C740-9E81-11CF-99D3-00AA004AE837}  Microsoft SendTo Service
   {7bafb3b1-d8f4-4279-9253-27da423108de}  WMV Screen decoder DMO
   {7bce3cfb-954c-438f-974c-73a8e0593f1a}  CClosableStreamWrapperProxy
   {7BD29E00-76C1-11CF-9DD0-00A0C9034933}  Temporary Internet Files
   {7BD29E01-76C1-11CF-9DD0-00A0C9034933}  Temporary Internet Files
   {7be73787-ce71-4b33-b4c8-00d32b54bea8}  HomeGroup Password
   {7be9d83c-a729-4d97-b5a7-1b7313c39e0a}  Programs Folder
   {7C021C10-E914-4A53-BDC8-315CEBF32B49}  CLSID_TrayToastActivator
   {7C07E0D0-4418-11D2-9212-00C04FBBBFB3}  MSPersist
   {7C127AC8-EC8D-40f2-91D0-B791CFC2397B}  Search Filter Kind Command
   {7C23220E-55BB-11D3-8B16-00C04FB6BD3D}  WM ASF Writer
   {7C2450CD-E430-4DAC-94FA-CEFAC1068505}  EventRetryParameter Class
   {7c27a1a1-0da5-45ac-a3d2-4fe7cb7a40e8}  Immersive Settings Cache Standalone object
   {7C28841A-AB97-498e-98C4-F6F143366FBC}  Proxy Credentials Page Class
   {7C48D08B-0DA5-4BA4-9C6E-4BB65DEB2005}  SplashScreen IconicBitmap
   {7c61d0a6-af7e-483a-b705-d2c5c2264656}  CLSID_EverywhereScopeFiller
   {7c67eb93-8eff-4e48-889f-45ba299bc46f}  Typed Data Thumbnail Handler
   {7c83c056-1d0d-4c8e-a6b0-89e79c213559}  Setup Cleanup Task
   {7C857801-7381-11CF-884D-00AA004B2E24}  PSFactoryBuffer
   {7C92505F-53A4-4D39-B31C-871D82A907DE}  PSFactoryBuffer
   {7cacbd7b-0d99-468f-ac33-22e495c0afe5}  Microsoft RDP Client Control - version 2
   {7CB359C5-570F-43c6-971F-1DB499EE57A1}  WMPlayer PlaybackPropPage Class
   {7cd3c903-d2e9-4a4d-8af3-3025445b24bf}  FilterControl
   {7CD4F369-6379-4EBB-86D4-87DA8E63CA3B}  Windows.ApplicationModel.Store
   {7CD6B491-C1A1-4F1C-B36E-A91B011DFADD}
BackgroundTransferCompletionGroupTriggerDetailsImpl
   {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}  Windows Search Manager
   {7D1933CB-86F6-4A98-8628-01BE94C9A575}  Virtual Disk Service
   {7D3195FF-A16A-43c3-9E50-E8A0975B234C}  BTHPAN Device Center Context Menu Handler
   {7d39c56f-6075-47c9-9bae-8cf9e531b5f5}  MF FLAC Sink Class Factory
   {7D559C10-9FE9-11d0-93F7-00AA0059CE02}  Code Download Agent
   {7D892F85-CC71-48fe-BFF6-72B7BD4F9C27}  NarratorGridItemPattern Class
   {7D8AA343-6E63-4663-BE90-6B80F66540A3}  VMR ImageSync
   {7DB7A939-E5C8-4eaa-B3E0-43CE04CAFFBE}
   {7db875bd-1b88-4c5f-9e4c-ed23eaff24e1}  Running Share Manager
   {7DE087A5-5DCB-4df7-BB12-0924AD8FBD9A}  WSMan InternalAutomation Class
   {7DED4D39-BE20-4AB6-983A-EB4ADCD9C93D}  CLSID_AppRepParm
   {7df2cfcd-6c09-415a-ae9d-5263f4964cbb}  SortColumnArray
   {7DF62B50-6843-11D2-9EEB-006008039E37}  Generate Still Video
   {7DF8EF76-D449-485f-B4EB-58DC96B31EDB}  HomeGroup Printing Device Class
   {7E08E268-CD23-4E97-B433-AB31D5BFB6AE}  Layout Manager
   {7E1A1FA9-EF4F-41E6-8F95-684ED50E039A}  Windows.Graphics.Printing.PrintManager
   {7e320092-596a-41b2-bbeb-175d10504eb6}  WMVideo8 Encoder DMO
   {7E37D5E7-263D-45CF-842B-96A95C63E46C}  Group Policy Object Proxy Stub
   {7E3FCEA1-31B4-11D2-AE1F-0080C7337EA1}  XML Viewer Moniker
   {7E48C5CF-72F6-4C84-9F43-B04B87B31243}  Scripting.Signer
   {7E4A23E2-B969-4761-BE35-1A8CED58E323}  XPS Thumbnail Generator
   {7e57f418-1f71-4411-9e09-45884f4f4714}  File Stream Marshaller
   {7e5fe3d9-985f-4908-91f9-ee19f9fd1514}
   {7E66DBEF-2474-4E82-919B-9A855F4C2FE8}  WscIsvIf Proxy Stub
   {7E8BC44E-AEFF-11D1-89C2-00C04FB6BFC4}
   {7e99c0a3-f935-11d2-ba96-00c04fb6d0d1}  ADs DN With Binary Object
   {7E9D8D44-6926-426F-AA2B-217A819A5CCE}  XML File Persistent Handler
   {7EB5FBE4-2100-49E6-8593-17E130122F91}  Fade Task
   {7ECBF017-BDC3-46D1-B9DA-95FA555D9ECF}  Windows Connected Search App Commanding
Provider
   {7ED25D63-48E5-4BE3-8539-3040B0B8991C}  Application View Broker
```

Page 73

SOFTWARE OUTPUT.txt

```
{7EE0A24E-A8C6-46ae-A875-8E7C3D18AEAF}   Favorites IFilter
{7efc002a-071f-4ce7-b265-f4b4263d2fd2}   Local Thumbnail Cache
{7f065fc8-efc7-4cab-82e0-694a14e910f2}
{7F12E753-FC71-43D7-A51D-92F35977ABB5}
{7F1899DA-62A6-11D0-A2C6-00C04FD909DD}   ScopeTree 1.0 Object
{7F1B9A54-8155-43BB-857C-461DAEFA46BD}   Device Discovery and Pairing Broker
{7F368827-9516-11D0-83D9-00A0C911E5DF}   Microsoft Server Configuration Notify
Object
{7F43B400-1A0E-4D57-BBC9-6B0C65F7A889}   PSFactoryBuffer
{7F4F2318-4AF6-432b-B957-B30D0779234E}   Sync engine info
{7F598975-37E0-4A67-A992-116680F0CEDA}   Microsoft WMI Provider Subsystem Self
Instrumentation
{7f5d25f8-78a5-49a8-a33c-2c0e11831c66}   WMDRM Context
{7F72CC7A-74A0-45B4-909C-14FB8186DD7E}   WBEM IP DFS Provider
{7F73B8F6-C19C-11D0-AA66-00C04FC2EDDC}
{7F75058C-9A21-4F22-A7CA-110205479EF9}
{7f8e7858-c362-4c0a-b868-4cdd929da715}   Authentication UI User Settings
{7F9CB14D-48E4-43B6-9346-1AEBC39C64D3}   MS Video Control Closed Captioning Feature
Segment
{7FB1D98A-F895-4761-8DC2-774969C84D10}   Win32_JobObject Provider Component
{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB}   WebCheck SyncMgr Handler
{7FC12E96-4CB7-4ABD-ADAA-EF7845B10629}   Authentication UI CredUI Out of Proc
Helper for AppContainer Clients
{7FE0D935-DDA6-443F-85D0-1CFB58FE41DD}   PSFactoryBuffer
{7febaf7c-18cf-11d2-993f-00a0c91f3880}   DefView Persistent history
{7FF0997A-1999-4286-A73C-622B8814E7EB}   ICodecAPIProxy
{80009818-f38f-4af1-87b5-eadab9433e58}   MF ADTS Property Handler
{802E19CB-06A0-445D-8297-7DFEEA406DDD}
{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}   WSecEdit Extension Class
{8066FB71-AFA1-343E-8070-44AB4F3F85C9}
{806f5b1a-d0db-4a89-94d8-c5712e796f9b}   DeviceAssociationBroker
{8078DA75-F43F-341D-A00E-20D6D736415E}
{807e5a10-4856-4f9a-8e3c-a1f7e75648b3}   CLSID_QueryResult
{8082C5E6-4C27-48ec-A809-B8E1122E8F97}   .contact shell extension handler
{8086ebd4-43e3-4b19-beb3-f0ea4ecf319c}   CScriptedDiagNativeHost
{8097A103-F7BC-4a17-876C-EE8446752464}   NarratorPattern Class
{8099904b-0b91-4906-a89d-11de2bd8f737}   StartMenu Path Complete Query Cache
{809B6661-94C4-49E6-B6EC-3F0F862215AA}   Collection of BDA Tuning Model
Components(Broadcast Substreams)
{80A09B21-11E7-462B-844A-1EB3415BB4A8}   CompressorServer.ProxyStubFactory
{80a90d72-a834-4f3d-ad3b-c7abbe4a0f66}   OOBE User Authentication
{80c68d96-366b-11dc-9eaa-00161718cf63}   Play command invocation
{80CB8C11-0E10-45F4-A1BA-EAD3838D7034}   Microsoft Virtual Disk Service Virtual
Disk Provider
{80D6C479-7B70-47DB-AECF-AB5480ADE1E5}   GlobalInterfaces Class
{80F3F1D5-FECA-45F3-BC32-752C152E456E}   Tablet PC Settings Control Panel
{80F94176-FCCC-11D2-B991-00C04F8ECD78}   MessageView Class
{80FCA77A-FBCB-4F7D-BC84-547E3F79D618}   CLSID_AccountPictureThumbnailHandler
{81007291-f070-4c4f-b978-ad1bec84babc}   Rename command invocation
{8101368E-CABB-4426-ACFF-96C4108120CD}   Plug and Play Provider Class
{810E402F-056B-11D2-A484-00C04F8EFB69}   CrSlide
{811F592B-CDE7-4ca4-A6D4-7BB3F60AD8FB}   Library Group Policy Shell Service Object
{81218F10-A8AA-44C4-9436-33A42C3852E9}   MSASR Locale Handler Class (1031)
{812F944A-C5C8-4CD9-B0A6-B3DA802F228D}   UIAnimationTransitionLibrary2
{8135397C-5C6C-4f6b-8E93-30685615F4EA}   DMS
{81397204-F51A-4571-8D7B-DC030521AABD}   DXTFilterFactory
{8144B6F5-20A8-444a-B8EE-19DF0BB84BDB}   StiEventHandler Class
{814B9800-1C88-11D1-BAD9-00609744111A}   VBI Surface Allocator
{814B9801-1C88-11D1-BAD9-00609744111A}   VideoPort VBI Object
{815E42F5-B141-45C2-B844-0BDFE9C558E2}
{8168e74a-b39f-46d8-adcd-7bed477b80a3}   MemoryDiagnosticTaskHandler
{81796171-DF5F-4F1B-A80C-BE4715D3C6BB}   TextNormMultiResult Class
{817F98C4-C9D9-4B8F-B8D0-413C8E5DBBB7}   BroadcastDVR Shell Component
```

Page 74

SOFTWARE OUTPUT.txt

```
{819469D2-D0CF-11d1-8E0B-00C04FC2E0C7}
{819d1334-9d74-4254-9ac8-dc745ebc5386}    InfoBar Manager
{81b43e73-e814-4dcd-a7c6-e22e7fe6a029}    Item Store Object
{81BD8EE8-F713-36A5-B7D5-9E92ACB4A18A}
{81CFA1FF-360D-4368-973A-670B8D2AA3B9}    User CPL User Manager Out of Proc Helper
{81d4e9c9-1d3b-41bc-9e6c-4b40bf79e35e}    CImeServerChs
{820825FD-1358-4705-8FEB-56B5CEE8BFD5}    NULL SSID INFO PAGE
{823535A0-0318-11D3-9D8E-00C04F72D980}    BDA Tuning Model Component Type Class
(Broadcast Substream Type)
{823B8267-735C-477E-8151-0FA9ADC8AB3A}    Convert ACL to SIDs and resolve SIDs
{82435bdf-f7c1-4df9-8103-eeabebf3d6e1}    WMDRM Content Enabler
{8278F931-2A3E-11d2-838F-00C04FD918D0}    Tracking Shell Menu
{827b7a93-2c48-433e-b247-8e3be20aab4a}    Group-by Column Explorer Command
{827CE1A1-8255-4165-8C83-8379F8C127AE}    Create and edit wireless policies
{82800303-1F33-402D-B832-052E23E9B7F9}    PSFactoryBuffer
{82A50877-57F6-4651-940A-8B557439F50C}    Notification Center Settings
{82BD0E67-9FEA-4748-8672-D5EFE5B779B0}
{82c588e7-e54b-408c-9f8c-6af9adf6f1e9}    FormatForDisplay Helper
{82d353df-90bd-4382-8bc2-3f6192b76e34}    WMVideo Decoder DMO
{82d792e9-8f8c-4f4a-9dbf-06253e4562a8}    FilterWorkerItem
{8336e323-2e6a-4a04-937c-548f681839b3}    X509 Certificate Template AD Writable
{833A69FB-5E17-4893-85A5-1EF469217372}    Wlan Radio Manager
{83472593-4fe6-4f44-a14c-fc8d4b4ff3f5}    Include In Library verb
{8368958c-a3ec-491f-9b4d-18f3f8287ee2}    IMEPREDICTPROP
{836932DD-FD20-4155-B781-DC3494D06C5A}    Foreground Manager
{8369AB20-56C9-11D0-94E8-00AA0059CE02}    Cleaner for Downloaded Program Files
{836CD085-B3D3-4b5c-BBCB-224F35EB0CCD}    Windows Push Notification Platform Keep
Alive Task
{836FA1B6-1190-4005-B434-7ED921BE2026}    UserDictionary Class
{8373ce97-72b7-4fb2-b5e8-b38aa083d734}    WinSync Anchor Provider Wrapper
{83781F70-1169-4489-A442-2C94FF328403}    Windows Package Setting Handler Factory
{838A77A6-14D4-439C-925F-30EE58005026}    CCOMNSScopeForExtensionSnapin Class
{8398EE59-134A-420A-934A-D86A7F900D9A}    IsdbString Class
{83B52078-E93E-425B-926F-DE6169875E41}    CLSID_AutoPlayUI
{83bb272f-7d5e-4b6e-9250-889893f0dac7}    Folder options command
{83bbcbf3-b28a-4919-a5aa-73027445d672}
{83BC5EC0-6F2A-11d0-A1C4-00AA00C16E65}
{83d6f579-4a45-439f-994e-7ec23c46b13e}
{83e05bd5-aec1-4e58-ae50-e819c7296f67}    PSFactoryBuffer
{83E94DBF-7F97-46B0-A6F0-360FE982BF83}    CLSID_TileElementFactory
{83F18638-2238-4B33-9FF8-24E759ADDC66}    SpPhraseBuilder Class
{8408B448-06CC-47A0-B482-BDAB666AF557}    Device Setup Status Extension
{840A0DD9-DC22-4f92-ABCE-894E6D8DCF47}    Audio Remote Endpoint Plugin Factory Class
{842a1268-6e6a-465c-868f-8bc445b9828f}    JScript Language
{842D84C9-C347-11D1-8F64-00C04FB611C7}    Interface Proxy Stub
{84302F97-7F7B-4040-B190-72AC9D18E420}    UIAnimationTransitionFactory2
{846225EA-B241-42A7-9D46-A694ECD5A781}    SpSharedRecognizer Class
{846727BE-C1B7-4A57-A638-A07264752C50}    PSFactoryBuffer
{84840C72-9913-4D9F-BEE4-447A8A875B82}    Microsoft Background Task Manager WMIv2
Provider
{8496e040-af4c-11d0-8212-00c04fc32c45}    AuStream Class
{84A3979A-6DD5-4a45-87B9-CBB47E0BF185}    NarratorRangeValuePattern Class
{84a3a6bf-f1d8-496e-9f05-d3de70973152}    WWan Helper Class
{84C050B8-8B00-409C-B752-6AFE92D9B812}    ImmersiveLauncherSearchMediator
{84C22490-C68A-4492-B3A6-3B7CB17FA122}    WalletDealsFactory
{84CCE1D2-97AD-4448-AF0F-A79164073A60}    Personalization Control Panel Element
Provider
{84D586C4-A423-11D2-B943-00C04F79D22F}    CustRg Class
{84e04a55-2d42-4909-86e3-62fd11483e8b}    Temporary Setup Files Cleanup
{84E65691-8602-4A84-BE46-708BE9CD4B74}    SoftwareBitmapNativeFactory
{84f0fae1-c27b-4f6f-807b-28cf6f96287d}
{84FC747A-1940-3D85-8819-EA53FC73DB1B}
{85074451-173D-4091-8648-C0E196BB363E}    WSUS App Publisher
```

Page 75

SOFTWARE OUTPUT.txt

```
{85076AB6-318F-4C72-AB29-8029D2CC28F9}  Bluetooth Rfcomm Device Access Capability
Handler Plugin
{8509bb76-ffa3-4827-ba5e-2e786010f42f}  Item Set Operations Object
{850D1D11-70F3-4BE5-9A11-77AA6B2BB201}  CommonDialog Class
{85131630-480C-11D2-B1F9-00C04F86C324}  JS File Host Encode Object
{85131631-480C-11D2-B1F9-00C04F86C324}  VBS File Host Encode Object
{85423CAE-A5E8-4AB4-BC89-D4FC6C283F63}
{854CB94F-2279-4F7F-AC62-31E22E4D8899}  InfraConnectTask
{855fec53-d2e4-4999-9e87-3414e9cf0ff4}  RunTask
{8570b44e-d109-42d3-be32-0f8d446669c5}  Close window command invocation
{8580ca99-925D-4537-959B-B7C9EA45FC01}  Shell Extensions
{85862EDA-F507-4d5b-ACA9-BB2C34A85682}  Microsoft XPS Rich Preview Handler
{858DACA2-78B4-412F-9A4E-315BBB4E1F21}  Open Command Prompt as Admin Command
{8596E5F0-0DA5-11D0-BD21-00A0C911CE86}  File Writer
{859AC360-A8F0-4d82-BBC7-7E28529FCC46}  DevInfoCSP
{85AFC315-CAC7-4475-875B-D7161BA14874}  SpInProcRecoContext Class
{85B3D708-4313-43F4-959B-829654791E8C}  Package State Handler Factory
{85BBD920-42A0-1069-A2E4-08002B30309D}  Briefcase
{85cfccaf-2d14-42b6-80b6-f40f65d016e7}  Shortcut
{85e94d25-0712-47ed-8cde-b0971177c6a1}  Microsoft DocProp Rating Control
{8601319a-d7cf-40f3-9025-7f77125453c6}  Sxs Store Class Proxy/Stub
{860d36ee-748e-4b73-ae45-c33187e6f166}  Microsoft IME Character Applet
{86151827-E47B-45ee-8421-D10E6E690979}  Closed Captions Analysis Feature Segment
{862321c3-70b2-4ee2-8231-87ec05819d98}  Transport Connection Helper Class
{863aa9fd-42df-457b-8e4d-0de1b8015c60}  Remote Printers
{863FA3AC-9D97-4560-9587-7FA58727608B}  SvcVwr 1.0 Object
{86422020-42A0-1069-A2E5-08002B30309D}  Network Context Menu Extension
{864A1288-354C-4D19-9D68-C2742BB14997}  User Event Timer
{864A9449-05B7-4A4F-B2FB-7CBACA74A5B1}  PSFactoryBuffer
{8652CE55-9E80-11D1-9053-00C04FD9189D}  DXRasterizer Class
{8653057E-8D73-4884-A5D1-4FCCCFFA542C}  LayerManagerState Class
{865e5e76-ad83-4dca-a109-50dc2113ce9a}  Programs Folder and Fast Items
{8664DA16-DDA2-42AC-926A-C18F9127C302}  PSFactoryBuffer
{8670C736-F614-427b-8ADA-BBADC587194B}  DirectShow Plugin Manager
{86747AC0-42A0-1069-A2E6-08002B30309D}  Briefcase Folder
{86bec222-30f2-47e0-9f25-60d11cd75c28}  Application Document Lists
{86c14003-4d6b-4ef3-a7b4-0506663b2e68}  Application Destination List
{86c815aa-4888-4063-b0ab-03c49f788be4}  OOBE OneDrive Optin
{86C86720-42A0-1069-A2E8-08002B30309D}  .exe drop target
{86d5eb8a-859f-4c7b-a76b-2bd819b7a850}  Virtual Factory for Usercpl
{86EB3FD8-E142-4f3d-B3D3-5D8F41097D58}  OOBE Misc Plugin
{86F80216-5DD6-4F43-953B-35EF40A35AEE}  CElevateWlanUi
{86FFEF81-E868-46F8-ACC2-290C2D8C3659}  DeviceUpdate CSP
{87099231-C7AF-11D0-B225-00C04FB6C2F5}  FaxTiff Class
{870AF99C-171D-4f9e-AF0D-E63DF40C2BC9}
{87170aa7-42d4-4999-8537-49e3d4ae0767}  CdsMetadata Class
{872f8dc8-dde4-43bd-ac7a-e3d9fe86ceac}  Windows System Reset SSO
{8732C40A-5572-4325-B989-094DD782D903}  CLSID_MIMERfc2047Encoder
{874131cb-4ecc-443b-8948-746b89595d20}  WMSpeech Decoder DMO
{8754DA31-5CF5-49c7-BDCF-C03045DA5A09}  WindowOpenedEvent Class
{87630419-6216-4ff8-a1f0-143562d16d5c}  Mobile Broadband Profile Settings Editor
{8770D941-A63A-4671-A375-2855A18EBA73}  InkRecognizerGuide Class
{877A0BB7-A313-4491-87B5-2E6D0594F520}
{877ca5ac-cb41-4842-9c69-9136e42d47e2}  File Backup Index
{878EC44B-7E5A-4e88-B688-7138196240C7}  NarratorMenu Class
{879795A1-A911-4FEF-984F-1A1CA4E14637}  Picture Password Image Setting Handler
{879fb53b-cba3-4fc8-b233-d9a93afa7fbc}  HomeGroup Task
{87AB8051-37BD-4e70-83C0-1E4F9AE1D37D}  Search MRU Command
{87BB326B-E4A0-4de1-94F0-B9F41D0C6059}  ThirdPartyEapDispatcherPeerRuntime
{87C8BA99-B13E-4BAE-87EE-E14A13172B26}  PrintWSDAHostStatics
{87CB4E0D-2E2F-4235-BC0A-7C62308011F6}  PSFactoryBuffer
{87D5FBE0-B972-450B-A488-5FE6347B45C8}  ContinousReadingEvent Class
{87D66A43-7B11-4A28-9811-C86EE395ACF7}  Indexing Options Control Panel
```

Page 76

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {87DB1ADA-AA39-11D1-829F-00A0C906B239} | |
| {87FC0268-9A55-4360-95AA-004A1D9DE26C} | DirectSoundWavesReverbDMO |
| {88004A5C-CEAC-41b9-A7A8-D5E166D32ACF} | NarratorProgressBar Class |
| {880ac964-2e34-4425-8cf2-86ada2c3a019} | State of play command |
| {882BC1E4-C79E-475D-8CC7-CC8D112FDB17} | RoamingSecurity Class |
| {883373C3-BF89-11D1-BE35-080036B11A03} | Summary Properties Page |
| {883FF1FC-09E1-48e5-8E54-E2469ACB0CFD} | SrControl Class |
| {8841d728-1a76-4682-bb6f-a9ea53b4b3ba} | LogonPasswordReset |
| {88445657-4A4E-4949-8FED-72B831C7C662} | MTF Input Type attributes |
| {884CFF4F-0BB0-4CAA-83BD-4FB9ECE938FA} | DefinitionLoader Class |
| {884e2000-217d-11da-b2a4-000e7bbb2b09} | ObjectId |
| {884e2001-217d-11da-b2a4-000e7bbb2b09} | ObjectId Collection |
| {884e2002-217d-11da-b2a4-000e7bbb2b09} | Binary Converter |
| {884e2003-217d-11da-b2a4-000e7bbb2b09} | X500 Distinguished Name |
| {884e2007-217d-11da-b2a4-000e7bbb2b09} | Csp Information |
| {884e2008-217d-11da-b2a4-000e7bbb2b09} | Csp Information Collection |
| {884e2009-217d-11da-b2a4-000e7bbb2b09} | Csp Status |
| {884e200b-217d-11da-b2a4-000e7bbb2b09} | X509 Public Key |
| {884e200c-217d-11da-b2a4-000e7bbb2b09} | X509 Private Key |
| {884e200d-217d-11da-b2a4-000e7bbb2b09} | X509 Extension |
| {884e200e-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Collection |
| {884e200f-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Key Usage |
| {884e2010-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Enhanced Key Usage |
| {884e2011-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Template Name |
| {884e2012-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Template |
| {884e2013-217d-11da-b2a4-000e7bbb2b09} | Alternative Name |
| {884e2014-217d-11da-b2a4-000e7bbb2b09} | Alternative Name Collection |
| {884e2015-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Alternative Names |
| {884e2016-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Basic Constraints |
| {884e2017-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Subject Key Identifier |
| {884e2018-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Authority Key Identifier |
| {884e2019-217d-11da-b2a4-000e7bbb2b09} | Smime Capability |
| {884e201a-217d-11da-b2a4-000e7bbb2b09} | Smime Capabilities Collection |
| {884e201b-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Smime Capabilities |
| {884e201c-217d-11da-b2a4-000e7bbb2b09} | Policy Qualifier |
| {884e201d-217d-11da-b2a4-000e7bbb2b09} | Policy Qualifier Collection |
| {884e201e-217d-11da-b2a4-000e7bbb2b09} | Certificate Policy |
| {884e201f-217d-11da-b2a4-000e7bbb2b09} | Certificate Policies Collection |
| {884e2020-217d-11da-b2a4-000e7bbb2b09} | X509 Extension Certificate Policies |
| {884e2021-217d-11da-b2a4-000e7bbb2b09} | X509 Extension MS Application Policies |
| {884e2022-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute |
| {884e2023-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Collection |
| {884e2024-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Extensions |
| {884e2025-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute ClientId |
| {884e2026-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Renewal Certificate |
| {884e2027-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Archivekey |
| {884e2028-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Archivekeyhash |
| {884e202a-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute OS Version |
| {884e202b-217d-11da-b2a4-000e7bbb2b09} | X509 Attribute Csp Provider |
| {884e202c-217d-11da-b2a4-000e7bbb2b09} | Cryptographic Attribute |
| {884e202d-217d-11da-b2a4-000e7bbb2b09} | Cryptographic Attribute Collection |
| {884e202e-217d-11da-b2a4-000e7bbb2b09} | Certificate Property |
| {884e202f-217d-11da-b2a4-000e7bbb2b09} | Certificate Properties Collection |
| {884e2030-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Friendly Name |
| {884e2031-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Description |
| {884e2032-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Auto-Enroll |
| {884e2033-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Request Originator |
| {884e2034-217d-11da-b2a4-000e7bbb2b09} | Certificate Property SHA-1 Hash |
| {884e2036-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Key Provider Information |
| {884e2037-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Archived |
| {884e2038-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Backed-Up |
| {884e2039-217d-11da-b2a4-000e7bbb2b09} | Certificate Property Enrollment |

Page 77

SOFTWARE OUTPUT.txt

```
{884e203a-217d-11da-b2a4-000e7bbb2b09}   Certificate Property Renewal
{884e203b-217d-11da-b2a4-000e7bbb2b09}   Certificate Property Archived Key Hash
{884e203d-217d-11da-b2a4-000e7bbb2b09}   Signer Certificate
{884e203f-217d-11da-b2a4-000e7bbb2b09}   Name Value Pair
{884e2042-217d-11da-b2a4-000e7bbb2b09}   X509 CertificateRequest Pkcs10
{884e2043-217d-11da-b2a4-000e7bbb2b09}   X509 CertificateRequest Certificate
{884e2044-217d-11da-b2a4-000e7bbb2b09}   X509 CertificateRequest Pkcs7
{884e2045-217d-11da-b2a4-000e7bbb2b09}   X509 CertificateRequest Cmc
{884e2046-217d-11da-b2a4-000e7bbb2b09}   X509 Enrollment
{884e2049-217d-11da-b2a4-000e7bbb2b09}   X509 Enrollment WebClassFactory
{884e204c-217d-11da-b2a4-000e7bbb2b09}   Certificate Property Enrollment Policy
Server
{884e2050-217d-11da-b2a4-000e7bbb2b09}   X509 Enrollment Helper
{884e2051-217d-11da-b2a4-000e7bbb2b09}   X509 Machine Enrollment Factory
{884e205e-217d-11da-b2a4-000e7bbb2b09}   X509 Certificate Revocation List Entry
{884e205f-217d-11da-b2a4-000e7bbb2b09}   X509 Certificate Revocation List Entry
Collection
{884e2060-217d-11da-b2a4-000e7bbb2b09}   X509 Certificate Revocation List
{884e2061-217d-11da-b2a4-000e7bbb2b09}   X509 Simple Computer Enrollment Protocol
{884e2062-217d-11da-b2a4-000e7bbb2b09}   X509 Simple Computer Enrollment Protocol
Helper
{8854F6A0-4683-4AE7-9191-752FE64612C3}   InkDivider Class
{8856918E-74C7-431C-B63D-3A5FDCC6AC08}   Microsoft Distributed Transactions
Coordinator WMI Provider
{8856F961-340A-11D0-A96B-00C04FD705A2}   Microsoft Web Browser
{886D29DD-B506-466B-9FBF-B44FF383FB3F}   EnhancedStorageSiloAction Class
{8872FF1B-98FA-4D7A-8D93-C9F1055F85BB}   ATSC Tune Request Location Information
{88753B26-5B24-49bd-B2E7-0C445C78C982}
{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}   Compressed (zipped) Folder SendTo Target
{889900c3-59f3-4c2f-ae21-a409ea01e605}   Shared Bitmap Object
{88A8465A-6789-4D8D-BACB-F3C1CDCE2E8F}   Composite Wireless Setting Handler
{88B02583-527D-43fa-B2C3-7A4C93D37C94}   NarratorHeaderItem Class
{88c524ca-551b-4c01-9a42-cdb16b745291}   ImeCommonAPI_JPN_Desktop_V1 Class
{88C6C381-2E85-11D0-94DE-444553540000}   ActiveX Cache Folder
{88d96a05-f192-11d4-a65f-0040963251e5}   XML DOM Document 6.0
{88d96a06-f192-11d4-a65f-0040963251e5}   Free Threaded XML DOM Document 6.0
{88d96a07-f192-11d4-a65f-0040963251e5}   XML Schema Cache 6.0
{88d96a08-f192-11d4-a65f-0040963251e5}   XSL Template 6.0
{88d96a09-f192-11d4-a65f-0040963251e5}   Free Threaded XML HTTP Request class 6.0
{88d96a0a-f192-11d4-a65f-0040963251e5}   XML HTTP 6.0
{88d96a0b-f192-11d4-a65f-0040963251e5}   Server XML HTTP 6.0
{88d96a0c-f192-11d4-a65f-0040963251e5}   SAX XML Reader 6.0
{88d96a0e-f192-11d4-a65f-0040963251e5}   SAXAttributes 6.0
{88d96a0f-f192-11d4-a65f-0040963251e5}   MXXMLWriter 6.0
{88d96a10-f192-11d4-a65f-0040963251e5}   MXHTMLWriter 6.0
{88d96a11-f192-11d4-a65f-0040963251e5}   MXNamespaceManager 6.0
{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}   Folder Redirection Editor
{890CB943-D715-401B-98B1-CF82DCF36D7C}   Volume Shadow Copy WMI Provider
{890F18BF-7246-4827-BC78-387C6980182A}   SettingsDatabase class
{89115307-8248-448f-ADA0-F3F3718A9B2A}   SystemAudioDeviceShared Class
{8929fd8a-3967-4896-a02d-f126195af6f7}   Shell Connected Accounts
{894132FE-635E-4F2F-B7AC-BB081636B1DB}   DevicesFlowBroker
{896664F7-12E1-490f-8782-C0835AFD98FC}   Libraries delegate folder that appears in
Users Files Folder
{896C2B1D-3586-4FA5-B419-41F4A6D38CF1}   SyncInfrastructureControl Class
{8973b4ef-7da5-4031-a333-f65609a4dcf4}   Search Everywhere Command
{898F8BC2-C6E3-4CD7-B04A-72E5B490B4C6}   MTF Suggestion Lattice Client
{89917B7C-A1A6-11DF-8BF6-18A90531A85A}   FhTaskHandler Class
{89AA9BF2-38EE-4444-8AE5-8CA90AAC64F6}   Bluetooth Generic Device Access Capability
Handler Plugin
{89BCB7A4-6119-101A-BCB7-00DD010655AF}
{89BCB7A5-6119-101A-BCB7-00DD010655AF}
{89BCB7A6-6119-101A-BCB7-00DD010655AF}
```

Page 78

SOFTWARE OUTPUT.txt

```
{89C2E132-C29B-11DB-96FA-005056C00008}  PBDA PTFilter
{89d1d0c2-a3cf-490c-abe3-b86cde34b047}  ReAgentTaskHandler
{89D83576-6BD1-4c86-9454-BEB04E94C819}  @%systemroot%\system32\mssvp.dll,-110
{89EA5B5A-D01C-4560-A874-9FC92AFB0EFA}
{89F2B8EB-AEDA-4057-A05B-A7D6181B63C6}
Windows.ApplicationModel.Core.RestrictedAppContainer
{8A01C400-A3E0-4F8D-A933-FF780F22BD87}  SnapinComponentData Class
{8A03567A-63CB-4BA8-BAF6-52119816D1EF}  Microsoft IMAPI Disc Recorder Enumerator
{8A03E749-672E-446E-BF1F-2C11D233B6FF}
{8A0A83A7-7A6D-48D6-8F3D-9029D8A76E06}  SettingSync Backup Manager
{8A11B5FA-3C92-4E8B-8382-3C71B757D679}  IE RSS Search Protocol Handler
{8A13B5B6-E5AE-467F-8C20-2968AFD886DC}  Bluetooth Gatt Device Access Capability
Handler Plugin
{8A22069C-1EF7-45D2-A409-219540D00A76}  Infrastructure Connect Page Class
{8A23E65E-31C2-11d0-891C-00A024AB2DBB}
{8A3E2E1E-A40B-4650-9FB4-30072A68E661}  ParseTracer Class
{8A44FFB7-8140-432F-BEC5-1B5FF725BAC8}  SpInprocRecognizer Class
{8A4D840D-AB27-4c8f-AB9C-765CA85C73B7}  Package installation state store
{8A667154-F9CB-11D2-AD8A-0060B0575ABC}  Microsoft DirectSound Wave
{8A674B49-1F63-11D3-B64C-00C04F79498E}  Utility Object for creating a Property Bag
backed by the Registry
{8A674B4C-1F63-11D3-B64C-00C04F79498E}  BDA Tuning Model Analog Radio Tuning Space
{8A674B4D-1F63-11D3-B64C-00C04F79498E}  BDA Tuning Model Analog TV Tuning Space
{8A6842BB-84DB-4EFA-99B9-06C850DF53FC}  WMPlayer NetworkPropPage Class
{8a696d12-576b-422e-9712-01b9dd84b446}  Status WMI Provider
{8A734961-C4AA-4741-AC1E-791ACEBF5B39}
{8a7cae0e-5951-49cb-bf20-ab3fa1e44b01}  Windows Font previewer
{8A89CB2C-1ED0-4709-A39C-FC34115DD660}  RDXHost
{8A95E9F1-1C07-4711-8DDA-10A35B26271E}  WorkspaceInstaller Class
{8A99553A-7971-4445-93B5-AAA43D1433C5}  OfflineActivation Class
{8A9B1CDD-FCD7-419c-8B44-42FD17DB1887}  UIAnimationTransitionFactory
{8ac3587a-4ae7-42d8-99e0-0a6013eef90f}  Device Proxy MFT
{8AC838A3-44C0-4015-A95E-CCAB02A3CFE2}  PSFactoryBuffer
{8ADBB9D2-2107-4044-9B63-0488124AD2F6}  ICS ConfigSP
{8ADD018C-5C5F-43C5-BE1E-07BAE85593B7}  HomeGroup Alpha Hosted Listener
{8ADE5386-8E9B-4F4C-ACF2-F0008706B238}
{8AE0163F-EDDD-4B0A-9C61-F7DD8B6137AE}
{8AE85776-D1E6-4043-A94C-1529D0E26E41}  NarratorSelectionPattern Class
{8aeff2c9-c97f-47b6-b27c-bd5969fe94d0}  CLSID_OOBEExperienceManager
{8AF662BF-65A0-4D0A-A540-A338A999D36F}  FaceCredentialProvider
{8b08efa2-bf11-4fa3-bbb4-655fb37c4fad}
Windows.Devices.Bluetooth.Background.RfcommConnectionTriggerDetails
{8B19C1CD-C80C-4AEC-AAE2-4E39FEDD24D0}  Microsoft Device Management Settings
Provider
{8b1f4c40-9d24-4427-b9fa-cc4388492394}  Windows.Devices.Custom Proxy
{8b20cd60-0f29-11cf-abc4-02608c9e7553}  WinNT Provider Object
{8b40abb8-6c65-465a-8c4b-26224df3125f}  Windows.Data.Pdf.ProxyStubFactory
{8b455e45-7cc8-4253-af5b-b2cd3313e9cc}  AppSync Setting
{8B7FBFE0-5CD7-494a-AF8C-283A65707506}  Default Location Class
{8B8C2776-594E-41EA-90D0-8013CACBB9A7}  Authentication UI CredUI Out of Proc
Helper for AppContainer Clients
{8B918B82-7985-4C24-89DF-C33AD2BBFBCD}  Microsoft RDP Client Control - version 10
{8BC3F05E-D86B-11D0-A075-00C04FB68820}  Windows Management and Instrumentation
{8BD9A7C7-6370-4A3C-A13F-6EA023A1E75C}  Microsoft Network Tuner Manager
{8be9f5ea-e746-4e47-ad57-3fb191ca1eed}  Listview Popup
{8BEBCE8B-1AF0-4323-8B4D-36994567CAE1}  Microsoft WMI Provider Subsystem InProc
Factory
{8bf9a910-a8ff-457f-999f-a5ca10b4a885}  V1 Smartcard Credential Provider
{8bfc4ca2-441f-4a4f-9891-4e6a6d5d2745}  Mobile Broadband Set Home Provider Page
Class
{8C0A1AC2-C6B3-447D-B971-35204B263972}  Windows Push Notification Download Task
Manager
{8C1645B0-9864-465E-BE75-990B030E4B11}  HomeGroup Task
```

Page 79

SOFTWARE OUTPUT.txt

```
{8C19ADE1-A894-4f78-BCB1-854A1464E442}  NarratorDataGrid Class
{8c2031f1-b169-4e7c-9cb0-56f18d7b0c01}  IAS XML Data Store
{8C334A55-DDB9-491c-817E-35A6B85D2ECB}
{8C38232E-3A45-4A27-92B0-1A16A975F669}  PSFactoryBuffer
{8C482DCE-2644-4419-AEFF-189219F916B9}  HostPeerApis
{8c4fb173-81ae-4399-9208-591a574a893f}  Mobile Broadband CFE Page Class
{8c4fb175-81ae-4399-9208-591a574a893f}  Pre-CFE Page Class
{8c4fce56-fc9a-4fcb-bd35-2ccabfd93844}  Authentication UI Logon Settings
{8c537469-1ea9-4c85-9947-7e418500cdd4}  ProtectedModeAPI
{8C7461EF-2B13-11d2-BE35-3078302C2030}  DEPRECATED: Component Categories cache
daemon
{8c7eaf13-fbd6-4ed8-ac79-fb12fcd71326}  SdEngine2 Class
{8C836AF9-FFAC-11D0-8ED4-00C04FC2C17B}  ReplicateCatalog Class
{8C89071F-452E-4E95-9682-9D1024627172}
{8C9E8E1C-90F0-11D1-BA0F-00A0C906B239}
{8CD34779-9F10-4f9b-ADFB-B3FAEABDAB5A}  .url File Persistent Handler
{8CD3AEA5-4B3B-4DE1-93EE-42BF9137194F}  Optimized Keyboard UI Class
{8cec58ae-07a1-11d9-b15e-000d56bfe6ee}  AP Client HxHelpPaneServer Class
{8cec58e7-07a1-11d9-b15e-000d56bfe6ee}  AP Client HxHelpPane Class
{8CF89BCB-394C-49b2-AE28-A59DD4ED7F68}  PSFactoryBuffer
{8D008BF5-038F-4D3D-A6F3-64CF62462D7E}  CallbackEventReporter
{8D04238E-9FD1-41C6-8DE3-9E1EE309E935}  MSVidCtl DVD to Audio Renderer Composition
Segment
{8d14113b-5715-4714-8a20-69fc343626de}  Multiplex Property Store
{8D1C559D-84F0-4BB3-A7D5-56A7435A9BA6}  Microsoft_WBEM WMI Object Factory
{8d1e5d4b-a99c-4408-b0f0-ccab9e5835a1}  SuggestFilterWorker
{8D4B04E1-1331-11d0-81B8-00C04FD85AB4}  CLSID_ImnAccountManager
{8D4D57E0-071A-42C7-A00A-14B3A91BE68F}  DLNAMetadataProvider Class
{8D6BABBD-C31E-4623-A400-A7668A26C864}  BMR Wifi Setting Handler
{8D759BEE-4828-47ad-9B19-F873D5E0F945}  OOBE Wireless Plugin
{8d80504a-0826-40c5-97e1-ebc68f953792}  OLE DocFile Property Handler
{8D86D59A-71BD-45A4-B2EB-8B240EB5F3A1}  App Pre-Install Task Manager
{8D8B8E30-C451-421B-8553-D2976AFA648C}  Sync Center Schedule Wizard
{8DA6DB1C-8114-40c6-9D97-D2E7E9757D67}  PSFactoryBuffer
{8DB0224B-3D65-4F6F-8E12-BEB4B78B8974}  MsAppx Scheme Handler
{8DB2180F-BD29-11D1-8B7E-00C04FD7A924}  COMComponentRegistrar Class
{8DBEF13F-1948-4AA8-8CF0-048EEBED95D8}  SpCustomStream Class
{8DE39096-D24E-4DF3-B24B-1B7F770BF799}  Explorer commands over a context menu
{8DE9C74C-605A-4acd-BEE3-2B222AA2D23D}  NegationCondition Class
{8E4062D9-FE1B-4b9e-AA16-5E8EEF68F48E}  Registration Control
{8E528C21-9D52-4030-BA92-3481227ADDD1}  WMPlayer PrivacyPropPage Class
{8E6E6079-0CB7-11d2-8F10-0000F87ABD16}  Offline Pages Cleaner
{8E757038-BE02-4bce-9680-E4BE0C6C70CD}  NarratorTextPattern Class
{8e827c11-33e7-4bc1-b242-8cd9a1c2b304}  Merged Folder Categorizer
{8e85d0ce-deaf-4ea1-9410-fd1a2105ceb5}  Microsoft DocProp Inplace Multi-Value
Property Control
{8E871B70-0F3D-4605-8919-89A7ACBA199C}  Global Rude Window Manager
{8e87e7b8-896b-4e67-bfa2-45c67d60ac3a}  CPL Search Target Services
{8E8F1601-AE98-3DAC-B48B-EC27C95A481E}
{8E908FC9-BECC-40f6-915B-F4CA0E70D03D}  Network and Sharing Center
{8E974B5A-A286-37DA-94F8-5872C500EB0E}
{8E989135-2736-4767-8160-EA3613F69D24}  IEDropSourceWrapper
{8EAD3A12-B2C1-11d0-83AA-00A0C92C9D5D}  DiskManagement.SnapInExtension
{8EB9BA6E-CEED-4D06-B7F6-EA6047221299}  CLSID_SearchSuggestionsService
{8ED392B6-23C2-4C3C-9126-D12D6BE621FD}  AppointmentDetailsActivationPlugin
{8EE97210-FD1F-4b19-91DA-67914005F020}  Microsoft DocProp Inplace ML Edit Box
Control
{8F0C5675-AEEF-11d0-84F0-00C04FD43F8F}  AthWafer
{8F22970F-2910-4baf-9B34-396F18318C17}  WmiCimV2ProfileAssociation
{8f3080a6-af99-4f2e-a806-f3d5702a0444}  Shell Computer Groups
{8F380D56-7ADE-449b-A748-D0F9595DBA6D}  AppEvtQProc Class
{8F5DF053-3013-4dd8-B5F4-88214E81C0CF}  SFP Repair Class
{8F60C6E5-0436-4B12-B53E-CA259BBD8868}
```

Page 80

SOFTWARE OUTPUT.txt

Windows.ApplicationModel.Contacts.ContactStoreNotificationTriggerDetails Factory
```
{8F914656-9D0A-4EB2-9019-0BF96D8A9EE6}
{8FA0D5A8-DEDF-11D0-9A61-00C04FB68BF7}
{8FADC6A8-183E-4DFC-944A-84A323334B98}   CFindNetPrinters Class
{8FD7E19C-3BF7-489B-A72C-846AB3678C96}   Smartcard Credential Provider
{8FD8B88D-30E1-4F25-AC2B-553D3D65F0EA}   DXP
{8FE3AA4C-4FFF-11E0-9EAE-3586DFD72085}   CLSID_StartMenuLauncherProvider
{8FF007D1-C3E3-44D5-86AF-2ECB5F663D7C}   IterableStringMarshalByValue
{8FF711AE-1954-4f87-B94B-3D8C4C50CAE4}   NarratorCalendar Class
{8FFE37E7-DDD3-434A-9DEB-1202D1BE31F7}
{90087284-d6d6-11d0-8353-00a0c90640bf}   Device Manager extension
{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}   DiagnosticInfrastructureCustomHandler
{900c0763-5cad-4a34-bc1f-40cd513679d5}   User Account Control Check Service
{901F6B1C-2FC6-4C28-BC8A-86C82765E96B}
```
Windows.Devices.Bluetooth.Background.BluetoothLEAdvertisementPublisherTriggerDetails
```
{90511715-D0AD-4DAA-A18B-254BD3AE1CF2}   FhSearch Class
{9052FC30-F3B5-49F7-91DB-9E78A2AB3900}
{9053699F-A341-429D-9E90-EE437CF80C73}
{905667aa-acd6-11d2-8080-00805f6596d2}
{9059f30f-4eb1-4bd2-9fdc-36f43a218f4a}   Microsoft RDP Client Control
```
(redistributable) - version 3
```
{905b55a8-77f0-4d28-80dd-e46b1412343f}   Execute OpenSearch view site command
{905FCFCB-7937-43CD-B0B1-95284CF8422E}   ContinuousReading Class
{9068BF36-6F05-477E-B108-A4042237F884}   OOBE UpgradeApps Wizard Page
{90903716-2F42-11D3-9C26-00C04F8EF87C}   SpCompressedLexicon Class
{90954C68-4D60-4023-A1F8-C6AF6F62E1C8}   Network and Sharing Center
{90AA3A4E-1CBA-4233-B8BB-535773D48449}   Taskband Pin
{90BA30DD-785C-4186-9F44-B7D2EA994EA5}   CApplicationWAPNodeProcessor
{90bd963c-925a-4628-b905-fa122a1890a6}   Microsoft IME Japan LM Suggestion Data
```
Source
```
{90BE9587-37b7-477C-81A7-BA7C5C40FF81}   MSASR Locale Handler Class (2057)
{90C69BBB-7F1D-4833-AF4E-87A7E5C4288B}   IME KOR Setting Handler
{90ED9FAA-A6E5-4671-8E50-1C060F8B9C47}   SFP Interface Class
{90F18417-F0F1-484E-9D3C-59DCEEE5DBD8}   CIeAxiInstallerService Class
{90F1A06E-7712-4762-86B5-7A5EBA6BDB01}   Microsoft Common Language Runtime Meta
```
Data V2
```
{90F1A06E-7712-4762-86B5-7A5EBA6BDB02}   Microsoft Common Language Runtime Meta
```
Data V2
```
{90f8c90b-04e0-4e92-a186-e6e9c125d664}   Property Labels
{9113A02D-00A3-46B9-BC5F-9C04DADDD5D7}   Enhanced Storage Data Source
{91145a83-a6c3-4181-89ff-8365f096f90d}   New Item Command
{9127081a-04b5-4044-b4c5-c7a9718e8795}   Help Command
{912A4CBA-0401-4631-91CF-5DDD3E3D6829}   An Entry for MTF Dynamic Dictionary Data
```
Source for Contacts
```
{912D9D84-DC73-48FA-8BD8-5315DE4B8FA8}
```
Windows.ApplicationModel.Email.EmailStoreNotificationTriggerDetails Factory
```
{913a6daa-57ee-4551-9ada-64d329d306a5}   App Locations Icon Extract Extension
{914feed8-267a-4baa-b8aa-21e233792679}   Microsoft Preview Creator
{91778246-9BE4-4713-A651-E833B853CC30}
{9185F743-1143-4C28-86B5-BFF14F20E5C8}   SpPhoneConverter Class
{91888BF6-FED1-4acd-9CB1-6C2F80AE58A3}
{9193A8F9-0CBA-400E-AA97-EB4709164576}   MSVidCtl SBE Source to Closed Caption
```
Composition Segment
```
{9197e04d-2b9f-4849-8bf7-75294eb5c043}   User Mode Bus Driver Class
{91ECFDB4-2606-43E4-8F86-E25B0CB01F1E}   ElevationConfig Class
{91f39027-217f-11da-b2a4-000e7bbb2b09}   X509 Enrollment Policy Active Directory
{91f39028-217f-11da-b2a4-000e7bbb2b09}   X509 Enrollment Policy Web Service
{91f39029-217f-11da-b2a4-000e7bbb2b09}   X.509 Policy Server List Manager Class
{91f3902a-217f-11da-b2a4-000e7bbb2b09}   X.509 Policy Server URL Class
{9200689A-F979-4eea-8830-0E1D6B74821F}   Virtual Factory for Recovery
{92038079-b9ef-428f-87f0-0463fcb1272a}   CLSID_VisibleIn
{9207d8c7-e7c8-412e-87f8-2e61171bd291}   Autoplay Known Devices Info
{920f80d3-5ef0-40dd-9a5e-eab11fcdf854}   CImeSearchIntegration Class
```
Page 81

SOFTWARE OUTPUT.txt

```
{92187326-72B4-11d0-A1AC-0000F8026977}  Game Controllers CPL Shell Extension
Default Property Sheets
{92192FD8-C1CB-434B-A8E8-B7F3AC424EE4}  OOBE PID Wizard Page
{92337A8C-E11D-11D0-BE48-00C04FC30DF6}  prturl Class
{92396AD0-68F5-11d0-A57E-00A0C9138C66}  RowsetHelper
{92498132-4D1A-4297-9B78-9E2E4BA99C07}  NSSManager Class
{924ccc1b-6562-4c85-8657-d177925222b6}  Desktop Gadget Helper API
{924DC564-16A6-42EB-929A-9A61FA7DA06F}  Authentication UI CredUI Out of Proc
Helper for Non-AppContainer Clients
{9264B7DC-A82F-4AFD-89C8-4F399DA7B028}  VAN Settings Page Class
{926749fa-2615-4987-8845-c33e65f2b957}
{926b23ab-fd60-43f1-8f63-b24cabdf5316}  View options command
{926f41f7-003e-4382-9e84-9e953be10562}  ADTS Byte Stream Handler
{9271B890-7BBF-48DB-ACB3-F973DC34156D}  PSFactoryBuffer
{927907E5-A066-4b07-BD4F-F53C7B748124}  WmiPowerMeter
{927971f5-0939-11d1-8be1-00c04fd8d503}  ADs Large Integer Object
{927ea2af-1c54-43d5-825e-0074ce028eee}
{928A906F-EADB-4EE2-8961-FE734AF257D1}  CloudExperienceHost API ProxyStub
{92A5010F-4404-4035-8D53-B87F5A736809}
{92A8CCF5-2725-4E95-9264-74FAB86FBBCA}  Cloud Change Wnf Monitor Class Factory
{92ab5af7-a374-417e-b2e2-9b317353a322}  Microsoft Library Boolean Check Mark
Control
{92ad68ab-17e0-11d1-b230-00c04fb9473f}  STClient Class
{92b66080-5e2d-449e-90c4-c41f268e5514}  G711 ACM Wrapper MFT
{92B94828-1AF7-4e6e-9EBF-770657F77AF5}  Custom Composition Segment from iTV to
Stream Buffer Source
{92BDB7E4-F28B-46A0-B551-45A52BDD5125}  PSFactoryBuffer
{92BF3D3E-E9D0-48a7-A459-98992E92A96B}  NarratorHeader Class
{92c85649-0892-4bc7-9b63-949f64149a26}  CMigrationPlugin Object
{92CC85F4-ACA4-4D72-94C8-49D1CAD0985F}  Infrastructure Connected Page Class
{92D2CC58-4386-45a3-B98C-7E0CE64A4117}  PSFactoryBuffer
{92dbad9f-5025-49b0-9078-2d78f935e341}  CLSID_PreviewMime
{92ED88BF-879E-448f-B6B6-A385BCEB846D}  MS Video Control Closed Captioning SI
Feature Segment
{9301E380-1F22-11D3-8226-D2FA76255D47}  DirectMusicContainer
{9305969B-F45F-47e5-A954-6EA879E874CC}  CPartitionSetPropPages Class
{93073C40-0BA5-11d2-A484-00C04F8EFB69}  CrInset
{9311A763-D284-4CE5-B2AA-6A99D9305D60}  Composite SettingHandler
{9324DA94-50EC-4A14-A770-E90CA03E7C8F}  Windows Theme Manager 2 API
{93412589-74D4-4E4E-AD0E-E0CB621440FD}  Font Settings
{9343812e-1c37-4a49-a12e-4b2d810d956b}  CLSID_SearchHome
{93443EB9-3F77-4DBE-84A2-D8467C1DD847}  RemovableMediaProvisioningPlugin
{93445657-12CA-4B80-AB18-9996D7293EC6}  MTF Lattice
{934A7048-1E4A-4D6E-9A9A-CB739F519B07}  HomeGroup Task
{934A9523-A3CA-4BC5-ADA0-D6D95D979421}  DirectPlay8Address Object
{934b410c-43e4-415e-9935-fbc081ba93a9}  UserInfoDialog
{934D4698-6A59-48f8-9F29-9FB30670320E}  Structured Query Helper Class
{935249A5-B5E8-43F6-A991-61435E5954B3}  Delete Address Bar History Command
{9357ffb2-0013-4c8e-9501-8e4e26f647d5}  CustomSystemTriggerDetails
{93714ED0-53F0-11D2-9EE6-006008039E37}  Frame Rate Converter
{937847E7-C78A-4834-9CE8-5F3EC99BD604}  Network Status Provider
{937C1A34-151D-4610-9CA6-A8CC9BDB5D83}  InkObject Class
{9381AF33-66A3-4D5A-8AF2-9515B1DC19A5}  PSFactoryBuffer
{939D20AC-8036-406F-BD5C-BF672896BD71}  View options gallery command
{93A094D7-51E8-485b-904A-8D6B97DC6B39}  SBE2 File Reader
{93a56381-e0cd-485a-b60e-67819e12f81b}  CLSID_CommonExplorerHost
{93AAD2A0-036A-4B11-A078-DA8776B38139}  HtmlLocalFileResolver
{93AC9CB8-27D5-4482-BFDF-68F21C7454A3}  Microsoft Shared Correction UI
{93AF0C51-2275-45D2-A35B-F2BA21CAED00}
{93CB110F-9189-4349-BD9F-392D9A4D0096}  Accessibility Control Panel
{93F7AA8E-CF82-4CB7-9251-48BC637A43B8}
{94291A92-7486-487B-BC9A-206A12880F02}  CLSID_LockAppHost
{94297043-BD82-4DFD-B0DE-8177739C6D20}  DMO Wrapper Filter
```

Page 82

SOFTWARE OUTPUT.txt

```
{942B7909-A28E-49a1-A207-34EBCBCB4B3B}   MSVidCtl Analog Capture to CCA Composition
Segment
{94357B53-CA29-4b78-83AE-E8FE7409134F}   Drive Size Categorizer
{9440861a-25ca-4bc2-833e-866a6191d110}   CLSID_SearchServicesProvider
{94426DE2-3211-11d2-A0DB-00C04F8EDCEE}
{944D4C00-DD52-11CE-BF0E-00AA0055595A}   DirectDraw Property Page
{94510291-3DB7-4F61-B62B-A5790CE92645}   Microsoft.WINDOWS.SQLLITE.Errors.4.0
{9456A480-E88B-43EA-9E73-0B2D9B71B1CA}
{94596c7e-3744-41ce-893e-bbf09122f76a}   Smartcard Pin Provider
{947812B3-2AE1-4644-BA86-9E90DED7EC91}   SpFileStream Class
{948B45F7-EFB8-46fb-8704-B340D847227A}   Location Description Property Handler
{948CFD8C-1888-4E52-8703-99610347EBB6}   AudioPump Class
{94971F89-D2EB-44ED-A217-A9BF27B74B65}
{94a909a5-6f52-11d1-8c18-00c04fd8d503}   Microsoft Group Extension
{94AB5C27-C954-4218-B0A1-29640412EFBE}
{94abaf2a-892a-11d1-bbc4-00a0c90640bf}   About Device Manager
{94B23D4D-1040-4C4B-9081-85D8D6FA36C4}   ImmersiveOpenWithUI
{94C00EC1-6E51-447A-87FA-8DF83767C155}   JScript Diagnostic Component
{94d86820-3128-41cd-be63-5e7bbd96a958}   TTLS Non EAP Interactive Task class
{94E03510-31B9-47a0-A44E-E932AC86BB17}   Windows Media Player Device Autoplay
{94E7F5BD-FC4F-446C-93D2-3942E8FE34C9}   Image Processor for Roaming
{94F35585-C5D7-4D95-BA71-A745AE76E2E2}   PSFactoryBuffer
{94FBC195-CB86-4142-9A6A-8E9CCF0D4F4D}   OOBE RetailDemo Plugin
{95158CD0-A5EE-4BEF-B9AC-8DE5D820275F}   CMusicSearchExecuteCommand
{95243A62-2F9B-4FDF-B437-40D965F6D17F}   VSSRemoteCoordinator Class
{95688ffa-250d-49bd-b40a-8ed3a8ef4c8e}   ImeKeyEventHandler Class
{956FADED-2450-4ABB-9F8C-4629FAFEBB92}   HomeGroup Listener Encryption
{95876EB0-90F0-11D1-BA0F-00A0C906B239}
{958A1709-3B44-11D1-AD74-00C04FC2ADC0}   RM Enlistment Helper
{958a6fb5-dcb2-4faf-aafd-7fb054ad1a3b}
{95CABCC9-BC57-4C12-B8DF-BA193232AA01}   WebAccount Object
{95CE8412-7027-11D1-B879-006008059382}   Shell Tree Walker
{960CE120-E284-45CE-83BC-A15B2EEE3DE8}   MTF Contact Harvester set up to use the
Contact Dynamic Dictionary Data Source
{961C1130-89AD-11CF-88A1-00AA004B9986}
{96236A71-9DBC-11DA-9E3F-0011114AE311}   PSFactoryBuffer
{96236A85-9DBC-11DA-9E3F-0011114AE311}   RdcLibrary Class
{96236A8F-9DBC-11DA-9E3F-0011114AE311}   SimilarityTraitsTable Class
{96236A90-9DBC-11DA-9E3F-0011114AE311}   SimilarityFileIdTable Class
{96236A91-9DBC-11DA-9E3F-0011114AE311}   Similarity Class
{96484065-846E-4C01-8D2A-44253F59B606}   Modern IME CHS Editing Model
{964A239F-6039-4A44-BB9B-EC0FEAFE28FC}   LegacyShareFields
{964ed064-ee96-4acf-972f-a40e5a2667d5}   SecondaryTileFlyout
{96709adb-52b9-4735-8534-3a8b32631432}   Windows.Security.Cryptography.Certificates
{96749373-3391-11D2-9EE3-00C04F797396}   SpResourceManager Class
{96749377-3391-11D2-9EE3-00C04F797396}   SpVoice Class
{9678f47f-2435-475c-b24a-4606f8161c16}   Microsoft Windows WSMan Provider Host
{968AD211-D1B1-444B-9F59-51701D1128D3}   psfactorybuffer
{9694E38A-E081-46ac-99A0-8743C909ACB6}   html persistent handler for mapi email
{96ac601f-ea2e-418b-94eb-bbc35b2ae7a8}   WinMDE MPEG2 SINK ACTIVATE
{96AC7453-0B2A-451e-9A1A-203CA034AF96}   Sync root make available online verb
{96AE8D84-A250-4520-95A5-A47A7E3C548B}   Parental Controls
{96B9DAE3-CF15-45e9-9719-57285348225E}   Windows Search OpenSearch Icon Handler
{96BEC059-2052-4e44-8E11-123ACDC936FE}   WMDM Sync Property Page
{96c7a5ef-0e2c-46d7-9bc1-6445c2444d7a}
{96f8e0d2-86e5-4898-8fb1-153682e11900}   PSFactoryBuffer
{97061DF1-33AA-4B30-9A92-647546D943F3}   WalletXFactory
{971127BB-259F-48c2-BD75-5F97A3331551}   Microsoft RDP Client Control
(redistributable) - version 3a
{973A7390-2608-3943-9015-D798D1217C08}
{973E4CE8-85A2-4207-8147-4778B50644DB}   Cloud Domain Join Authentic User Gesture
{9743B50B-3190-4061-8DA3-BE13AA02181E}   Infrastructure Progress Page Class
{974C63D2-6846-4F6B-BF27-BF71ADB1E608}   Print Platform Compat
```

Page 83

SOFTWARE OUTPUT.txt

```
{975797FC-4E2A-11D0-B702-00C04FD8DBF7}
{975ABEDC-F64B-436d-ABFF-44B932459856}   Windows Media Player OCXAdvancedPropPage
Class
{97B35842-B010-4910-99AF-EED43B123BF4}   WpcSync Provider Class
{97d47d56-3777-49fb-8e8f-90d7e30e1a1e}   Work Folder Logon Trigger Class
{97e467b4-98c6-4f19-9588-161b7773d6f6}   Office Document Property Handler
{98037168-078f-4e5a-b235-a41aa5fd3bf5}   WMPMDE MPEG2 SINK ACTIVATE
{98042251-8C2B-4FC4-93E2-B1DB331EF5B9}   WMPlayer AdvancedPropPage Class
{98068995-54d2-4136-9bc9-6dbcb0a4683f}   Microsoft Windows Remote Shell Host With
User Settings
{9821D278-84E2-4D6A-8712-2C6E23D43C7B}   EnterpriseModernAppMgmtCSP
{98230571-0087-4204-b020-3282538e57d3}   Color Converter DMO
{98455561-5136-4d28-AB08-4CEE40EA2781}   MF Video Presenter
{984F9804-3314-4FA4-AC8C-E688D4133C51}   Workspace Setup Confirm Settings Page
{9877D8A7-FDA1-43F9-AEEA-F90747EA66B0}   KernelTraceProvider Class
{987D8DFA-3E2C-4929-9C51-61AC8E00CBC3}   Shell Logged On Accounts
{98859A6C-02F2-43FC-ADB0-CE6D10F1A1AA}
{9885AEF2-BD9F-41E0-B15E-B3141395E803}
{989D1DC0-B162-11D1-B6EC-D27DDCF9A923}   XML Script Engine
{989F13EE-B25B-4FAB-9AED-C4336C8CCF0C}   MtfTransportServerDCOM
{98A1B01E-E363-46e9-A68F-C6078DAABB8C}   W7TODMSCONVERTER.2.0
{98A238A9-D8A2-4E57-84AF-6CF88FF719DA}   Notify Cloud Change
{98af66e4-aa41-4226-b80f-0b1a8f34eeb4}   Manifest mime handler
{98AFF3F0-5524-11D0-8812-00A0C903B83C}   CertRequest Class
{98F275B4-4FFF-11E0-89E2-7B86DFD72085}   CLSID_StartMenuLauncherProviderFolder
{98F63271-6C09-48B3-A571-990155932D0B}   FaxControl Class
{98FF6D4B-6387-4b0a-8FBD-C5C4BB17B4F8}   IE MRU AutoComplete List
{9909aba6-519d-4b42-b57f-cc1408214ddb}   User Name Format
{990a9f8f-301f-45f7-8d0e-68c5952dba43}   Shell Create Object Task Delegate
{991DA7E5-953F-435B-BE5E-B92A05EDFC42}   MSVidCtl Stream Buffer Source To Generic
Sink Composition segment
{992CFFA0-F557-101A-88EC-00DD010CCC48}   Network Connections
{99325BBE-E0A7-48A1-A23E-716582D09FEF}   CConnectedSearchExecuteCommand
{995C996E-D918-4a8c-A302-45719A6F4EA7}   Shell Hardware Mixed Content Handler
{9970407f-eb6c-40bc-96d4-6e8b69b2017f}   PSFactoryBuffer
{99793286-77CC-4B57-96DB-3B354F6F9FB5}
{99847C33-B1B4-11D1-8F10-00C04FC2C17B}   CCOMNSScopeImpl Class
{99969a8f-27e6-4adf-ab9f-b5b5e90d4733}   Verb Handler for launching verbs on
properties of items
{99a73266-0cdf-4479-88af-1842cbaada22}   IImeIPointSrv wrapper class
{99acf7f6-ef55-4ef9-8e27-3b784a6b4639}   Shell Positioner Manager
{99B29D3B-368A-4BE6-B675-805A69114497}   UserMarshal
{99c0179c-c20c-488c-a510-bd779b9376ae}
{99CDC6E0-DA00-4dfa-8EB8-831D774F8891}   Shell Profile Accounts
{99cdfdaf-3573-4d97-bc06-d7c36627edef}   Mobile Broadband Connect Failure Page
Class
{99D353BC-C813-41ec-8F28-EAE61E702E57}   Share With Verb
{99D54F63-1A69-41AE-AA4D-C976EB3F0713}   VMR Allocator Presenter
{99d6470e-d780-4fce-99d2-40324846c10b}   CTransactedMemPropertyStoreProxy
{99E89F48-A745-416d-A4E0-ECF53C65DFA0}   DynamicRenderer Class
{99EB9580-04EC-4B4C-99F5-52B616D444D9}   MSASR Locale Handler Class (1031)
{99F997ED-DFD1-4F67-B367-9B52B8225A85}   MCCS CalDavSyncEngine
{9a010fcc-488b-4836-94fd-c489f8e1ed7d}   NDIS Helper Class
{9a02e012-6303-4e1e-b9a1-630f802592c5}   Packed Property Storage Object
{9a07804e-7050-41d5-a244-badc038df532}   Library Restore Defaults verb
{9a096bb5-9dc3-4d1c-8526-c3cbf991ea4e}   IE RSS Feeds Folder
{9a2584c3-f7d2-457a-9a5e-22b67bffc7d2}   psfactorybuffer
{9A3E1311-23F8-42DC-815F-DDBC763D50BB}   WalletAimProxyFactory
{9A43A844-0831-11D1-817F-0000F87557DB}   Compositor
{9A4948D9-13FC-4FAC-B60A-FBA6EE0FB11C}   SLSClient
{9A4A4A51-FB3A-4F4B-9B57-A2912A289769}   Blinds
{9A4B1918-0A2F-4422-89DD-35B3F455999C}
{9A4B942C-C16D-44D2-BDAA-1BD772A4050B}   SpTextSelectionInformation Class
```

Page 84

SOFTWARE OUTPUT.txt

```
{9A5EA990-3034-4D6F-9128-01F3C61022BC}   GameExplorer Class
{9A653086-174F-11D2-B5F9-00104B703EFD}   Microsoft WBEM WBEM Class Object
{9A7C3FC6-8C9E-40A8-8CD9-0F3715483825}  ·PSFactoryBuffer
{9a97f12a-6b73-4dc4-b3c1-e9244c03adac}   shell foreground window setter
{9AA0422B-E5C5-4A6B-ACEC-C96E2E05B353}   CIsdb Class
{9aa46009-3ce0-458a-a354-715610a075e6}   Sync Integration Manager
{9ab3b1c9-3225-4bb4-93b6-bfb3c0d93743}   Disc Image Mount
{9AB6A28C-748E-4B6A-BFFF-CC443B8E8FB4}   Microsoft ALAC Audio Encoder MFT
{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}   ShellItem Shell Namespace helper
{9acf41ed-d457-4cc1-941b-ab02c26e4686}   Microsoft Windows WSMan Provider Host With
User Settings
{9AED384E-CE8B-11D1-8B05-00600806D9B6}   WBEM Scripting Named Value Collection
{9B0EFD60-F7B0-11D0-BAEF-00C04FC308C9}   Temporary Internet Files Cleaner
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}   CAutoUpdate Class 1.0
{9B39403C-8B6D-430D-AE71-9EE1DC6E74C5}   Background Uploads Monitor
{9B39610A-38D1-43f1-9FAF-D4E5CA50B4B2}   NarratorEdit Class
{9B467978-A0CF-480B-965B-5A5FAC1D8277}   MouseMonitor Class
{9b4e5207-9539-4258-b4a0-4e70e9e565ec}   User Accounts Control Panel
{9B55AA0E-1BC2-46e4-B306-DF9BDFDCC644}
{9B77C0F2-8735-46c5-B90F-5F0B303EF6AB}   CAsfTocParser
{9B78F0E6-3E05-4A5B-B2E8-E743A8956B65}   RDPSession Class
{9B8C4620-2C1A-11D0-8493-00A02438AD48}   DVD Navigator
{9B97D384-048C-4e24-926D-DB6F0841C9E4}
{9BA05971-F6A8-11CF-A442-00A0C90A8F39}   Microsoft Shell Folder View Router
{9BA05972-F6A8-11CF-A442-00A0C90A8F39}   ShellWindows
{9BC773B8-9B6C-400F-8AF0-0DFDD1C43229}   SpVoice Class
{9BCE6E2B-116B-420F-928B-5356D1629979}
{9BF8D948-5C56-450e-BAF8-D6144C6E81CB}   SqlGenerator Class
{9C07355E-C50A-45D2-B4A3-0A8235F8047F}   CommandStore Action Handler
{9c15e692-86da-4ab8-8b5e-6ac79deb6f20}   Desktop Positioner
{9C1CC6E4-D7EB-4EEb-9091-15A7C8791ED9}   InkRenderer Class
{9c212ed3-cfd2-4676-92d8-3fbb2c3a8379}   AppReadiness Service Class
{9C33C4AB-BC91-4A79-BF47-7C90CEBC3AA3}   Switch Controller
{9C38ED61-D565-4728-AEEE-C80952F0ECDE}   Virtual Disk Service Loader
{9C483F92-DAD8-437d-9D0D-C8F64A6815AD}   CLSID_AppSpaceXMLParser
{9C49FB9B-4E8C-43AE-BACF-76404B422264}   DSC TIMER
{9C502F01-0D36-4f16-8AC9-8693E0D84E44}   WMPlayer CDBurnPropPage Class
{9C60DE1E-E5FC-40f4-A487-460851A8D915}   AutoPlay
{9C62D90D-9C14-400a-942A-404ABA5E1F38}   CWapDPUHelper
{9C649633-9D4E-40A5-9F0A-32C35D9D6FE3}   Windows Connected Search Query Suggestion
·Provider
{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF}   Sync Center Folder
{9c7a1728-b694-427a-94a2-a1b2c60f0360}   ShdocvwBroker
{9C86F320-DEE3-4DD1-B972-A303F26B061E}   PSFactoryBuffer
{9c8db22b-8ddc-471c-9628-48847514b424}   WCM Policy APIs
{9CAB4470-D6FA-4903-986C-7D5A755B2691}   RoamingSecurity Class
{9cb233a5-a4a5-46b9-ab13-db07ce949410}   Password retry UI class
{9CB5172B-D600-46BA-AB77-77BB7E3A00D9}
{9CB90915-45B8-4427-A49A-3CCD929FD859}   ContextManager
{9CC1CC97-48C6-43DB-8265-4BD9C8E192DD}
CAppointmentsProviderInternalReplaceAppointmentActivationPlugin
{9cca66bb-9c78-4e59-a76f-a5e9990b8aa0}   Drive Cleanup Command
{9CD64701-BDF3-4D14-8E03-F12983D86664}   BDA Tuning Model DVB Terrestrial Locator
{9CDAEA40-A7D3-4cc5-AED0-B5E35AD0F169}   SpW3CSemanticInterpretation Class
{9CE31F69-2605-420C-A30E-B60A164DB44D}
Windows.ApplicationModel.Chat.ChatMessageNotificationTriggerDetails Factory
{9cfc2df3-6ba3-46ef-a836-e519e81f0ec4}   Property System Apartment Class Factory
{9cfc6d75-e648-47a8-9ea0-fb0907558952}   DTC Transaction List Control
{9d06f027-cbfc-421a-97b3-f09a8a9359bc}   OnDemandBrokerExecutorProxy
{9D079FE7-A102-4F3F-AD2E-A2C88C851CEE}   CellularSettingPublisherInternal
{9D148290-B9C8-11D0-A4CC-0000F80149F6}   Microsoft InfoTech Protocol for IE 3.0
{9D148291-B9C8-11D0-A4CC-0000F80149F6}   Microsoft InfoTech Protocols for IE 4.0
{9D27B916-4F17-4EE8-A71C-D84222993D64}   CellularAPI_OEM
```

Page 85

SOFTWARE OUTPUT.txt

```
{9D3C0751-A13F-46a6-B833-B46A43C30FE8}  MAPI Shell Context Menu
{9D71A98F-1E45-42EC-AF3D-FA13BEFB955C}  Limited Connectivity Page Class
{9D745ED8-C514-4D1D-BF42-751FED2D5AC7}  HNetCfg.FwProduct
{9D958C62-3954-4b44-8FAB-C4670C1DB4C2}  IE Microsoft Shell Folder AutoComplete
List
{9D99BE80-B271-4524-BA35-30414FE18F0E}  PrintWSDAHostPrxy
{9DA3DFB6-DB99-4A52-B52B-058E0C6B7956}  MSASR Locale Handler Class (2057)
{9DB7A13C-F208-4981-8353-73CC61AE2783}  Previous Versions
{9DBD2C50-62AD-11d0-B806-00C04FD706EC}  Property Thumbnail Handler
{9DCC3CC8-8609-4863-BAD4-03601F4C65E8}  LatLongReportFactory Class
{9DCCCE22-C057-424E-B8D1-67935988B174}  HealthAttestationCSP
{9DD35758-AAF5-4894-ADAA-77A492F54E0A}  WlanDlgNonUIPage Class
{9DE85094-F71F-44f1-8471-15A2FA76FCF3}  InkWordList Class
{9df523b0-a6c0-4ea9-b5f1-f4565c3ac8b8}  Date and Time Properties
{9E175B68-F52A-11D8-B9A5-505054503030}  Search Gathering Manager
{9E175B69-F52A-11D8-B9A5-505054503030}  Search Embedded Gathering Manager
{9E175B6C-F52A-11D8-B9A5-505054503030}  Search Gatherer Transaction
{9E175B6D-F52A-11D8-B9A5-505054503030}  Search Gatherer Notification
{9E175B6E-F52A-11D8-B9A5-505054503030}  Microsoft Embedded Search Gatherer
Notification
{9E175B70-F52A-11D8-B9A5-505054503030}  Search Gatherer Language Resource Pool
{9E175B74-F52A-11D8-B9A5-505054503030}  Search Gatherer Plug-in
{9E175B76-F52A-11D8-B9A5-505054503030}  Windows Search Service File Protocol
Handler
{9E175B7F-F52A-11D8-B9A5-505054503030}  Search Back off Controller
{9E175B8A-F52A-11D8-B9A5-505054503030}  Search command creator object
{9E175B8B-F52A-11D8-B9A5-505054503030}  Windows Search Data Source
{9E175B8D-F52A-11D8-B9A5-505054503030}  Search FilterRegistration Class
{9E175B8E-F52A-11D8-B9A5-505054503030}  Search LoadLangRes Class
{9E175B90-F52A-11D8-B9A5-505054503030}  Full Text SQL Parser
{9E175B98-F52A-11D8-B9A5-505054503030}  Search Neutral Word Breaker Resources
{9E175BA8-F52A-11D8-B9A5-505054503030}  Search Null Word Breaker
{9E175BA9-F52A-11D8-B9A5-505054503030}  Search Gatherer Log File Provider
{9E175BB7-F52A-11D8-B9A5-505054503030}  Windows Search Service Tripoli Indexer
Engine
{9E175BB8-F52A-11D8-B9A5-505054503030}  Windows Search Service Jet Property
Storage Engine
{9E31421C-2F15-4F35-AD20-66FB9D4CD428}
System.EnterpriseServices.RegistrationHelperTx
{9E358D23-02B2-4CCD-9FEE-6B75EE8DD5CA}  PSFactoryBuffer
{9E51E0D0-6E0F-11d2-9601-00C04FA31A86}
{9E56BE60-C50F-11CF-9A2C-00A0C90A90CE}  Mail Service
{9E56BE61-C50F-11CF-9A2C-00A0C90A90CE}  Desktop Shortcut
{9E704F44-90F0-11D1-BA0F-00A0C906B239}
{9e752621-4573-4308-81c6-9f210db29e85}  Optimize Library For verb
{9E77AAC4-35E5-42A1-BDC2-8F3FF399847C}  Stream Buffer Sink Segment
{9E797ED0-5253-4243-A9B7-BD06C58F8EF3}  iTV Playback Feature Segment
{9EB7C6FC-0C96-4EE0-9B8A-F4BDA7D305E1}  DataPackagePropertySetPrivate
{9EBB177D-0161-4e2c-81B0-E15D586CFC9F}  PSFactoryBuffer
{9EC4B4F9-3029-45ad-947B-344DE2A249E2}  Urlmon Scheme Handler
{9ecb380c-2333-4c68-9691-a569fe446820}  MAPISendMailServer
{9ecf51f8-cfb1-458d-9485-f5a231afd22f}  CLSID_XMLAutoList
{9ECF752A-518E-46b1-8691-F5090F5E9A14}  Linguistic Alternative Generator
{9ED4692C-90F0-11D1-BA0F-00A0C906B239}
{9ED96B20-73AA-11D2-952C-0060081840BC}  Frame Rate Converter Property Page
{9ED96B21-73AA-11D2-952C-0060081840BC}  Audio Repackager Property Page
{9ED96B22-73AA-11D2-952C-0060081840BC}  Dexter Queue
{9EE72A18-7BD4-44E1-8BA9-1E8E60D8CCA3}  Microsoft WDAC WMI-v2 Provider
{9EF96870-E160-4792-820D-48CF0649E4EC}  SpAudioFormat Class
{9EFD4CF2-0BAA-350B-9D73-0974077B2F7B}
{9f2b0085-9218-42a1-88b0-9f0e65851666}  Windows SmartScreen Task Handler
{9F36C194-166C-4cbf-B7EA-BF039F950172}  PeerGroup Wrapper
{9F377D7E-E551-44f8-9F94-9DB392B03B7B}  CProvideWinSATVisuals Class
```

Page 86

SOFTWARE OUTPUT.txt

```
{9f37f39c-6f49-11d1-8c18-00c04fd8d503}   Microsoft PrintQueue Extension
{9F4F643B-8806-4861-8A79-6699E94DCF66}   Preferred HomeGroup Changed XML
{9F50E8B1-9530-4DDC-825E-1AF81D47AED6}   MSVidCtl Analog TV to StreamBufferSource
Composition Segment
{9F66347C-60C4-4C4D-AB58-D2358685F607}
{9f75fdc4-0aba-4866-88a9-75ebb9e7d584}   CImeCommandAvailabilityView_JK Class
{9F8E6421-3D9B-11D2-952A-00C04FA34F05}   Glow
{9FAE1230-74AC-4e33-B59C-4051BBEB0803}   IE Thread Handshake
{9fb45d27-dfe3-4383-b117-ab631787649a}   Picture Password Task Handler
{9FC8E510-A27C-4B3B-B9A3-BF65F00256A8}
{9FD4E808-F6E6-4e65-98D3-AA39054C1255}   InkRecognizers Class
{9FE63AFD-59CF-4419-9775-ABCC3849F861}   System Recovery
{9ff13758-469b-45a8-8cc7-72182bd7e9ba}   Microsoft IME SKF Applet
{9FF65B15-F7B4-4858-BFE6-DB2083DEDF68}   SpObjectToken Class
{9ff7242c-364d-425d-95ce-c64f8ee140d1}   Mobile Broadband Puk1 Page Class
{a00e1768-4a9b-4d97-afc6-99d329f605f2}   CPartitionNotify Class
{a00ee528-ebd9-48b8-944a-8942113d46ac}   CLSID_StartMenuCommandingProviderFolder
{a015411a-f97d-4ef3-8425-8a38d022aebc}   CLSID_FindExecute
{A0202464-B4B4-4b85-9628-CCD46DF16942}   Move-To Choose Folder
{A0275511-0E86-4ECA-97C2-ECD8F1221D08}   Infrared
{A02797FC-C4AE-418C-AF95-E637C7EAD2A1}
{a028ae76-01b1-46c2-99c4-acd9858ae02f}   IMKRTIP
{A03FB29D-1AF8-4632-9778-2DE93E21A4F1}   AEP Setting Monitor
{A05AD39D-C5E6-4723-8802-AB7788548580}   Shell Publishing XML
{a07034fd-6caa-4954-ac3f-97a27216f98a}   Query file associations
{A08AF898-C2A3-11d1-BE23-00C04FA31009}   Windows Mail Envelope
{A0953C92-50DC-43bf-BE83-3742FED03C9C}
{A09CCA86-27BA-4F39-9053-121FA4DC08FC}
{A0A7A57B-59B2-4919-A694-ADD0A526C373}   Tearless Window Presenter
{A0A8C450-92FC-422a-AA04-0A19E8D65AC7}   TypeAhead Local Metadata Provider
{A0B9B497-AFBC-45AD-A8A6-9B077C40D4F2}   Custom Composition Segment from Encoder to
Time Shift Sink
{A0CAF057-8D9E-4d01-8CDD-5F469B153A9F}   NarratorList Class
{a0d018ee-1100-4389-ab44-464faf001288}   Authentication UI Logon Sound
{A0D465BE-92E9-4340-A5FE-5ACD9A67EB79}   RenderTextEvent Class
{A0F8D82C-E4D8-4ED9-BD3A-867A830B12BA}
Microsoft.Windows.DataProtection.Adapters.DpProviderFactory
{A0F93E27-F05D-4153-A151-F3720369A4C7}   Microsoft WMI Signed Driver Provider
{A1006DE3-2173-11d2-9A7C-00C04FA309D4}   CLSID_COE5Import
{a1019a03-1281-47b1-93bc-856d5f0cda43}   Windows.Devices.AllJoyn.ProxyStubFactory
{a10dfc9e-ff12-4e7f-bc74-8fe9053920f0}   WinSync Full Enumeration Provider Wrapper
{A1103531-6B1C-425F-A8C9-671616E40FA9}
{A1170F2C-C5A4-467F-8EB3-50571D7201AE}   Mouse Setting Handler
{a11850eb-4501-4dea-9ef5-1d37f57d247d}   Mobile Broadband Create Profile Page Class
{A11DB3DC-5FF6-4a0b-AEE6-29BCAC1E11E0}
{A1230201-1439-4E62-A414-190D0AC3D40E}   PSFactoryBuffer
{A1230401-67a5-4df6-a730-dce8822c80c4}
{A12E5BCB-9758-4FBE-9B85-F50C822E6B5E}   EnterpriseAppMgmtClient
{a1570149-e645-4f43-8b0d-409b061db2fc}   Provides methods for enumerating paired
MTP over Bluetooth devices
{A167B942-CD17-4d00-BDD9-8FDC2DC158F2}
{a16e1bff-a80d-48ad-aecd-a35c005685fe}   IMA ADPCM ACM Wrapper MFT
{A17DA8D0-F67D-47A0-9EC4-19C486383206}   IP Security Monitor
{A188DB29-2ABC-46cb-9A38-40B82CF5D051}   CLSID_HomeGroupCollectionServer
{A19141CE-D197-4C8B-82C9-4995F5303497}   Projection UI
{A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980}   Collection of BDA Tuning Model Component
Types(Broadcast Substream Types)
{A1B1922F-B626-4A4F-9F2B-4A6926DF86D1}   Output Manager Class
{A1B9E04A-3226-11D2-883E-00104B2AFB46}   SDSnapin Description
{A1BFB370-5A9F-4429-BB72-B13E2FEAEDEF}   ICMFilter
{a1e2b86b-924a-4d43-80f6-8a820df7190f}   IMKROTIP
{A1E48442-883D-491A-BE68-41214236D6A8}
Windows.System.SystemManagement.ProxyStubFactory
```

Page 87

SOFTWARE OUTPUT.txt

```
{A1E7036D-72A1-4529-B108-0C3C9E92D424}  Create and edit Wired policies
{A1EBDBD0-E4BA-4DB3-8DF6-C91534061EF4}  Audio Flyout Controller
{A1F4E726-8CF1-11D1-BF92-0060081ED811}  WIA Device Manager
{A1FC5C0F-6A66-4858-8BA5-1E467D09695D}  Running Share Manager SIHost Component
{A21FC522-F671-4013-9339-0828E5C70DD9}  FocusChangedEvent Class
{A22C4FC7-6E91-4e1d-89E9-53B2667B72BA}  MF MPEG4 Sink Class Factory
{A25821B5-F310-41BD-806F-5864CC441B78}  WlanPref LUA
{A258718D-BE3E-40CC-A77F-75642516497C}
{A26CEC36-234C-4950-AE16-E34AACE71D0D}
{A28798CC-730B-41EB-9CA2-74F93E27B99E}
{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}  Start Menu Pin
{A2D75874-6750-4931-94C1-C99D3BC9D0C7}  Microsoft Windows Defender
{A2D8CFE7-7BA4-4bad-B86B-851376B59134}  Windows Parental Controls
{A2DC4FCB-C32A-4E4E-A2DB-67A008913992}  AppointmentActivation ProxyStubFactory
{A2E3074E-6C3D-11D3-B653-00C04F79498E}  BDA Tuner Device Segment
{A2E30750-6C3D-11D3-B653-00C04F79498E}  BDA Tuning Model ATSC Tuning Space
{A2E6DDA0-06EF-4df3-B7BD-5AA224BB06E8}  ImageFile Class
{a3037d66-c043-4f54-91a0-2cdb642e7718}  IMETip
{A31AD6C2-FF4C-43D4-8E90-7101023096F9}  Time Synchronization Task Handler
{a31c0e24-c249-4e36-a1a3-9dfdceda9bbc}  EAPTLS Identity UI class
{a323554a-0fe1-4e49-aee1-6722465d799f}  DateTimeCPL Flyout Class
{A32552C5-BA61-457A-B59A-A2561E125E33}  UPnPDevice Class
{A3367904-52A3-4A11-BF5B-1AB36EF51D1F}  Windows.Internal.Management
{A3401FFE-D67C-46b6-BAD8-77D091223EC6}  NarratorPasswordElement Class
{A35C5B62-6032-4CAF-BB23-F0556BFF94FF}  SmRecipient
{A373F500-7A87-11D3-B1C1-00C04F68155C}  Windows Search Service Client Side Cache
Protocol Handler
{A37B2DFB-4204-4476-B1D9-29413836093D}  Shell User Domain Enumeration Object (by
groups)
{a38b883c-1682-497e-97b0-0a3a9e801682}  IPropertyStore Handler for Images
{A38E6420-19EC-490c-B4BF-51673C360213}  Search Filter More Properties Command
{a38f3677-32fc-4dac-99b3-d804b193d2c4}  ImeKeyEventHandler Class
{A38F4597-F640-4189-982F-132ECF8202FA}  WPDSyncProvider Class
{a3b3c46c-05d8-429b-bf66-87068b4ce563}  Security and Maintenance Notification
Manager
{A3BC03A0-041D-42E3-AD22-882B7865C9C5}  Microsoft RDP Client Control - version 9
{a3c3d402-e56c-4033-95f7-4885e80b0111}  Previous Versions Results Delegate Folder
{A3C97737-76D9-4f5f-B917-4DE47FE023C8}  CWinsatWMI Class
{A3CCEDF7-2DE2-11D0-86F4-00A0C913F750}  CoPNGFilter Class
{A3D93AB0-3079-4662-BF03-1718156E7C32}
{A3E41207-BE04-492A-AFF0-19E880FF7545}  WMI instrumentation:
Win32_ComputerShutdownEvent
{A3ECBC41-581A-4476-B693-A63340462D8B}  Filter Graph Private Thread
{a405dda4-a05a-46be-b481-526ad2e0c791}  CImeDictAPIWebServiceComment Class
{A4109FA5-7512-4338-8376-81F6D38ADA41}  CloudExperienceHost Environment Default
Implementation
{A4173A49-F373-4475-9A0F-2D615204DC20}  Network State Change Task Handler
{a41a4187-5a86-4e26-b40a-856f9035d9cb}  Microsoft Terminal Services Client Control
- version 1
{a42c2ccb-67d3-46fa-abe6-7d2f3488c7a3}  Windows RTF Previewer
{A43139B3-BDF5-4497-9DCF-6C7AADC1A5D0}  MusDialogHandler
{A43C525D-EDF0-48d9-B7FB-9BABBD6DBD65}  Windows Setting Handler Factory
{A4445657-BCB6-476E-8336-3A2ACD96E299}  MTF Suggestion Input Lattice Query
{A45AEC2B-549E-405F-AF3E-C6B03C4FDFBF}  ToggleDMRAuthorization
{A470F8CF-A1E8-4f65-8335-227475AA5C46}  Encryption Context Menu
{a47286bf-d624-4a30-acdf-2705bd3de0c3}  WinMDE LPCM SINK ACTIVATE
{a47401f6-a8a6-40ea-9c29-b8f6026c98b8}
{A47979D2-C419-11D9-A5B4-001185AD2B89}  Network List Manager
{a479ddb1-2166-40d0-8fb0-892687d2fa12}
Windows.Networking.Sockets.SocketActivityTriggerDetails
{A47C0430-EDBD-464E-A2AF-3B17C26AFDF5}  DragDropEvent  Class
{A4B07E49-6567-4FB8-8D39-01920E3B2357}  Virtual Factory for Windows Firewall Cpl
{A4B544A1-438D-4B41-9325-869523E2D6C7}  TF_CategoryMgr
```

Page 88

SOFTWARE OUTPUT.txt

```
{a4c31131-ff70-4984-afd6-0609ced53ad6}   Shell ChkdskEx Dialog
{A4DDCA2B-E73C-40C5-83B1-9F40269D0B0D}   OnlineActivation Class
{A4E05936-2251-4634-B684-09D5122A8F72}   VaultSettingsHandler Class
{a4f0da76-0f57-495f-bb5d-9f67a4745cdf}   GameListEntryProxy
{A4F2A5C9-979A-4EC6-851F-341F15D3F67D}   FhProgressDialog Class
{a4fbcbc6-4be5-4c3d-8ab5-8b873357a23e}
{A5065670-136D-4FD6-A45F-00C85B90359C}   DsmAdminControl Class
{A508E5FE-7D8F-4006-AE92-A44E69F87DA3}   MtfTransportServerDCOM Core
{a5183349-82de-4bfc-9c13-7d9dc578729c}   CStorageFolderProxy
{A5270F6C-19EC-4E17-9EA1-A7074276B9B9}   Windows Search Items Changed Sink
{A530D54A-DBA0-4b17-9F99-51A7A2CC17CA}   Tethering Setting Handler
{a542e116-8088-4146-a352-b0d06e7f6af6}   Address EditBox
{A55803CC-4D53-404c-8557-FD63DBA95D24}   WPDShextAutoplay
{A58845F3-BC16-4689-883F-68A15916B660}   CloudExperienceHost Broker User Operations
Implementation
{A5B020FD-E04B-4e67-B65A-E7DEED25B2CF}   TabletManager Class
{A5EAE54D-9886-4B8D-AA78-EAFF38D011CA}   CLSID_ResetEASPolicies
{A5EBA07A-DAE8-4d15-B12F-728EFD8A9866}   PSFactoryBuffer
{A5EFE073-B16F-474f-9F3E-9F8B497A3E08}   PSFactoryBuffer
{A5FA505C-DB54-403c-A744-9B3919EF096F}   Windows.Media.Streaming
{A608A731-B6F2-4d08-AC1E-C22A65B64ACF}   Explorer Separator Band
{A6098E79-9C50-4F87-8973-5FB4532C93D8}   BTConnectionUi Class
{A61DDE94-66CE-4AC1-881B-71680588895E}
{A6207B2E-7CDD-426A-951E-5E1CBC5AFEAD}   PSFactoryBuffer
{A6358B41-04B3-477F-B8E5-7EDB1A5D7ACD}   Visual Element Event Dispatcher
{A63E13D5-5263-44A6-8A18-381EB6F181A2}   SpMMAudioIn Class
{A6439333-78D2-4FFD-A20D-53B0EDC704BA}   AppSync Setting Monitor
{a6482830-08eb-41e2-84c1-73920c2badb9}   Removable Storage Devices
{A64CAF32-08CD-4054-BFD5-983BEDA9264A}   WebProviderTokenRequest Object
{A65B8071-3BFE-4213-9A5B-491DA4461CA7}   DxDiagProvider Class
{a671c915-d95d-4135-b2c3-089356ca694f}   Nla Helper Class
{a677570a-2ba2-4e9a-b2e2-8a02cd8b4fd3}   CoPrintIsolationHost Class
{A6787DB4-F958-4938-855B-594534865351}   Immersive Print Dialog
{A680CE8D-9CA7-43BF-B41E-5066973215AB}   CloudExperienceHost Broker User Operations
Default Implementation
{A68B20E5-0E4B-4E79-8310-FEF1912C9C66}   IP Sender Data Plugin
{a6914418-134b-4bb8-8e3d-7fef7f456caf}   CRasDiagHelper Object
{A6B222AB-A5EA-4899-B230-084657EDDC7D}   Browser Thread State
{A6BFEA43-501F-456F-A845-983D3AD7B8F0}   Virtual Factory for MaintenanceUI
{A6EE35C6-87EC-47DF-9F22-1D5AAD840C82}
{A6F1684D-AED6-401b-9786-A3E3B53C6641}   Parental Controls Control Panel
{A73BEEB2-B0B7-11D2-8853-0000F80883E3}
{a76de978-f3eb-4a4f-9f99-304ad619e2ab}   State of OpenSearch view site command
{A79020BC-1F7E-4D20-AC2A-51D73012DDD5}   MSASR Locale Handler Class (1040)
{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}   Secure Startup
{A7AA4814-7479-4047-BC99-32E757C8B850}   FhSearchNotifySite Class
{A7B9649E-FECE-4AE3-958C-C36B133E937F}
{A7C06739-500F-4E8C-99A8-2BD6955899EB}   PSFactoryBuffer
{A7C452EF-8E9F-42EB-9F2B-245613CA0DC9}   Windows Defender WMI Provider
{a7c922a0-a197-4ae4-8fcd-2236bb4cf515}   Microsoft Feeds LoRi Broker
{A7D04CE0-9FDE-4E03-9AB2-1DD9255BEE9C}   PrintDialog.ProxyStubFactory
{A7EE7F34-3BD1-427f-9231-F941E9B7E1FE}   DXTFilterCollection
{A8040703-2640-48B7-96CD-BC8108A4E8F1}   SnapinComponent Class
{A8159411-398E-4471-9521-A84B0BF2BE54}   Device Setup UI DSM Task Class
{A8159420-398E-4471-9521-A84B0BF2BE54}   Device Setup UI Details Page Class
{A8159421-398E-4471-9521-A84B0BF2BE54}   Device Setup UI Error Handling Page Class
{A82E50BA-8E92-41eb-9DF2-433F50EC2993}   MP3 Byte Stream Handler
{A83EF168-CA8D-11D2-B33D-00104BCC4B4A}   CLSID_IntProv
{a842a6e3-2bac-436f-bb7e-5645f65c01fc}   PSFactoryBuffer
{A860CE50-3910-11d0-86FC-00A0C913F750}   CoDitherToRGB8 Class
{a86ca2f1-af74-4a74-980b-e185d4ca01b0}   HomeGroup Wizard Finished Page
{A8792A31-F385-493C-A893-40F64EB45F6E}   PSFactoryBuffer
{A879E3C4-AF77-44fb-8F37-EBD1487CF920}   PSFactoryBuffer
```

Page 89

SOFTWARE OUTPUT.txt

```
{A87FA4A8-339A-48f3-A9B5-44CB8CFEF3F7}  MCCSAutdManager
{A89003D7-25F1-47fd-B504-6B35E7A63A27}
{a893aa73-054f-4dbc-9e53-f4ee5fe07fd3}  Cached File Updater Merge Handler
{A894CA92-2E31-4AF2-BC7E-41079A8E5BE9}  Immersive Monitor Notification Service
Proxy
{A896FD50-87BE-449A-9149-D10BA1FAAEE2}  LockScreen Call Broker Factory
{A8976A00-1FDE-4B5F-A6F0-FBF459DD32ED}  AppContractPolicy
{a8a881fb-bee9-4cdf-b052-ae42e427e319}  Fingerprint Settings Handler
{A8A91A66-3A7D-4424-8D24-04E180695C7A}  Device Center
{a8c3476d-20e1-4d56-96e7-84e24952228b}  UserDicManager Class
{A8C680EB-3D32-11D2-9EE7-00C04F797396}  SpMMAudioOut Class
{A8CA4495-65AB-4333-9FF9-4FEB6FBF5169}  App URI Resolver
{a8cc4a39-8f83-44eb-a73e-e2848c4f585f}  WMPMDE RTSP SINK ACTIVATE
{A8CD0ADC-23D6-4B79-BCC9-D3309DF34760}  Access Page Setting SSO
{A8CDFF1C-4878-43be-B5FD-F8091C1C60D0}
{a8d93b39-2113-492e-b014-801d01c95eca}
{A8DCF3D5-0780-4EF4-8A83-2CFFAACB8ACE}  BDA Tuning Model ATSC Component Type Class
(Broadcast Substream Type)
{A8DFB9A0-8A20-479F-B538-9387C5EEBA2B}  VMR Mixer 9
{A8E64375-B645-4314-9EFC-C085981786FA}
{A910187F-0C7A-45AC-92CC-59EDAFB77B53}  SpObjectTokenCategory Class
{A919EA73-490E-4D5C-9BA7-97CBC73119FE}  Immersive Settings Cache
{A91DEAA6-9773-42B7-86A4-5AD24CFF440A}  SMB Witness Service CIM provider
{A9224722-48E4-4A66-8068-F90FA13A6D74}  User Tile Setting Handler
{A9249952-F4C6-4BCD-9B44-6A5BA9B5209E}  Immersive App Execute Open Verb
{A9397D66-3ED3-11D1-8D99-00C04FC2E0C7}
{A961F842-FC8E-4D53-8074-4AB67E8854B4}
{A9710FB5-1840-4224-BD42-86831E28E43A}  RemMdmObj Class
{A973E7B2-131B-428E-8B2B-EAE73D731E98}  Security and Maintenance Notification
Activator
{A989DC2B-5E13-4426-9BD4-F666D96F15F8}  WMDRM Plugin
{A9927F85-A304-4390-8B23-A75F1C668600}  Token Provider
{A9A33436-678B-4c9c-A211-7CC38785E79D}  WinSAT Task Manger Task
{a9ae6c91-1d1b-11d2-b21a-00c04fa357fa}  LW Identities
{A9B005E5-AB63-4C1D-AE9E-AA120A50BB0F}  Lock Screen Slideshow Manager
{A9B48EAC-3ED8-11d2-8216-00C04FB687DA}  Content Indexer Cleaner
{A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}  Search Gatherer Inline Notification
{a9bdbb2f-8b01-455a-917f-0acf7b4a4a24}  dmwmicsp
{A9C3BF62-4524-4989-8AA9-DE019D2E551F}  PSFactoryBuffer
{A9CF0EAE-901A-4739-A481-E35B73E47F6D}  Microsoft DocProp Inplace Edit Box Control
{a9d7038d-b5ed-472e-9c47-94bea90a5910}  Microsoft RDP Client Control
(redistributable) - version 8
{A9F738C8-6B96-41FA-A155-15ECD67275D0}  Windows Search Protocol Handler Search
Connector Creator
{A9FC132B-096D-460B-B7D5-1DB0FAE0C062}  RMGetLicense Class
{AA000926-FFBE-11CF-8800-00A0C903B83C}  CertServerPolicy Class
{AA04CA0B-7597-4F3E-99A8-36712D13D676}  LicensingStateTools Class
{AA0EB6FC-A8EB-4FD9-A861-0014B374076E}  AppSync Setting Handler
{AA10385A-F5AA-4EFF-B3DF-71B701E25E18}  Wordpad ODT Document Filter
{aa1b0e54-7593-40a0-8135-ed0b6cbc0154}  Media Foundation MPEG2 MUX MFT Activate
{aa28fbc7-59f1-4c42-9fd8-ba2be27ea319}  Select All command invocation
{AA2E2C5B-0B0C-4ECC-B32B-3935269E0588}  HomeGroup CPL Command
{AA453FDC-5D6C-4C33-AD14-67680BF6F1DD}  DMAccNodeProcessor.1.0
{AA49497A-AD46-46f7-A5E0-7C9E76543B99}  CLSID_NotificationElementFactory
{aa509086-5ca9-4c25-8f95-589d3c07b48a}
{AA527A40-4D9A-11D2-93AD-00805F853771}  Microsoft NT DS Instance Provider for WBEM
{AA558FA2-A340-4a23-B765-614BA827CE1D}  SppInstallerFactory Class
{AA65DD7C-83AC-48C0-A6FD-9B61FEBF8800}  Delivery Optimization Mgmt Class
{AA67AF38-4AE0-4B49-BA56-ADF78DBED45A}
CAppointmentsProviderInternalRemoveAppointmentActivationPlugin
{AA70DDF4-E11C-11D1-ABB0-00C04FD9159E}  Microsoft WBEM View Provider
{AA7E3C50-864C-4604-BC04-8B0B76E637F6}
{AA87D6C0-777A-4483-B5BF-07B8668B2225}  CMiracastSourceInputManager
```

Page 90

SOFTWARE OUTPUT.txt

```
{AA94DCC2-B8B0-4898-B835-000AABD74393}
{aaa0d501-ec92-4c17-a930-90dd0d2f6c95}   Windows.Media.Editing
{AAA288BA-9A4C-45B0-95D7-94D524869DB5}   WPDShServiceObj Class
{AAB9C730-3C6C-4faa-A87E-77198D9E2A57}   Event Record XML
{AABE54D4-6E88-4c46-A6B3-1DF790DD6E0D}   Themes tree item callback object for
sysdm.cpl
{AABFB2FA-3E1E-4A8f-8977-5556FB94EA23}
{aac1009f-ab33-48f9-9a21-7f5b88426a2e}   TSRDSettings Class
{AAC2B978-266D-48ae-AA28-60A3EBB872D0}   IE RSS FeedFolder Tasks
{AAC46A37-9229-4fc0-8CCE-4497569BF4D1}   InkRecognizerContext Class
{AAC85F70-3395-4F9B-A609-D625A2F07CEF}   E-Ink
{AAD3DECB-03A4-4DF6-821F-F8A1357EB25D}   NowPlayingSessionManagerStatics Class
{aad40095-d757-481d-8b7b-b60fbbe67b7f}   CSearchContactExecuteCommand
{AADFA891-4F4D-46E6-BF6B-E9A260931A01}
{ab0b37ec-56f6-4a0e-a8fd-7a8bf7c2da96}   CLSID_ExplorerHostCreator
{AB0D8B78-D7F8-4249-AC86-3A3E3D7BFBC4}   ChtChangjieDS
{AB1890A0-E91F-11D2-BB91-00C04F8EE6C0}   SpMMAudioEnum Class
{AB2ECE69-56D9-4F28-B525-DE1B0EE44237}   PSFactoryBuffer
{AB300F71-01AB-46D2-AB6C-64906CB03258}   Media Foundation MPEG2 MUX MFT
{AB3B125A-120F-4444-B5EB-E14738782758}   Windows Connected Search Music Provider
{ab3d00ba-f2dd-4deb-b122-177b161ead5b}   StoreAgent
{AB40A5C1-804B-40BD-9DFE-A640691C6956}   Win32_JobObjectSecLimitInfo Component
{AB517586-73CF-489c-8D8C-5AE0EAD0613A}   Microsoft DocProp Custom Draw Percent Full
Control
{AB540CD3-2E37-450D-A095-D0651D9C379F}   KeyboardEchoEvent Class
{AB790AA1-CDC1-478a-9351-B2E05CFCAD09}   CPartitionContextMenu Class
{AB7BC55E-4BD8-430E-ADB2-D29A5DA20624}   RTMediaFrame
{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}   Thumbnail Cache Class Factory for Out of
Proc Server
{AB93B6F1-BE76-4185-A488-A9001B105B94}   BDEUILauncher Class
{AB944620-79C6-11D1-88F9-0080C7D771BF}   Event Publisher
{ABB27087-4CE0-4E58-A0CB-E24DF96814BE}   InertiaProcessor Class
{ABBA0005-3075-11D6-88A4-00B0D0200F88}   ATSCTerrestrial Class
{ABBA0006-3075-11D6-88A4-00B0D0200F88}   CDvb Class
{ABBA001B-3075-11D6-88A4-00B0D0200F88}   DigitalCable Class
{ABBB0332-21FC-4F9A-BBF0-C329B38611D9}
{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE}   Subscription Mgr
{ABCA6774-29B5-4aff-A776-C2551AE0FFE6}   Image Sanitization Broker
{abd2ad24-f1ff-47ad-82de-3a1edf38e7a1}   HomeGroup Task
{ABDBD0B1-7D54-49fb-AB5C-BFF4130004CD}   PSFactoryBuffer
{ABE40035-27C3-4A2F-8153-6624471608AF}   MSVidCtl Digital TV to StreamBufferSource
Composition Segment
{abeb77d3-f67a-4e33-a412-86b310bc274e}   Windows.Media.Protection.PlayReady
{AC3315C9-F481-45D7-826C-0B406C1F64B8}   Microsoft Dolby Digital Encoder MFT
{AC3AC249-E820-4343-A65B-377AC634DC09}   V1 WinBio Credential Provider
{AC48FFE0-F8C4-11d1-A030-00C04FB6809F}   RequestMakeCall Class
{AC4CE3CB-E1C1-44CD-8215-5A1665509EC2}
{AC75D454-9F37-48f8-B972-4E19BC856011}
{ac7d68a4-c4e5-450f-a89b-d630b25bb996}   Microsoft IME Japan LM Suggestion Data
Source
{AC7ED533-3E39-4350-A0E3-CCB7D8043825}   IFindInstalledAppInfo.ProxyStub
{AC82FF6D-E524-4c0f-8D0B-0C74C1ECAAEA}   InkCursors Class
{ACA965C4-D406-4531-B6D9-C099D5D8EDEA}   App Transition Manager
{ACA97E00-0C7D-11d2-A484-00C04F8EFB69}   CrSpiral
{ACB77480-075F-4093-A47F-23C7C1377780}   Device Discovery and Pairing Broker
Provider
{ACC56A05-E277-4B1E-A43E-7A73E3CD6E6C}   DeviceBroker
{ACD453BC-C58A-44D1-BBF5-BFB325BE2D78}   Microsoft MPEG-2 Audio Encoder
{ACD71912-705E-4C3E-90BD-14F31595D361}   Windows.Help.Runtime.HelpFilter
{ACE52D03-E5CD-4b20-82FF-E71B11BEAE1D}   Shell Name Space ListView
{ace575fd-1fcf-4074-9401-ebab990fa9de}   Microsoft RDP Client Control - version 4
{AD325995-B74D-41E4-A240-C472A50D41C2}   PSFactoryBuffer
{AD4C1B00-4BF7-422F-9175-756693D9130D}   PSFactoryBuffer
```

Page 91

SOFTWARE OUTPUT.txt

```
{AD581B00-7B64-4E59-A38D-D2C5BF51DDB3}  WindowsMediaLibrarySharingServices Class
{AD5FBC96-ACFE-46bd-A2E2-623FD110C74C}  NarratorButton Class
{AD6B3B23-C74A-4B2C-839F-C1149CB42E7F}  PSFactoryBuffer
{AD6C8934-F31B-4F43-B5E4-0541C1452F6F}  WST Pager
{AD7572AD-86A5-4211-BC54-A438E550A740}  Application PreLauncher
{ad763fa6-3b90-41ab-bd44-4f832beee55f}  Windows Media Network Source Plugin
{AD76E74F-F730-4813-BF9F-BD139C13E9BF}  NarratorGroup Class
{AD7B5554-C683-4C04-AAF9-9676822D2692}
{AD8E510D-217F-409B-8076-29C5E73B98E8}  Stream Buffer Source
{ad974ae2-e292-4083-a280-0342d68daf55}  Updatable Item Set
{ADAB9B51-4CDD-4af0-892C-AB7FA7B3293F}  Group Policy Service User Profile
Notification
{adacedf4-9c34-430e-a65f-488f0ab491da}
{ADB880A4-D8FF-11CF-9377-00AA003B7A11}
{ADB880A6-D8FF-11CF-9377-00AA003B7A11}  HHCtrl Object
{ADB9F5A4-E73E-49b8-99B6-2FA317EF9DBC}  Windows ScreenSaver Properties
{ADBDEF00-9A50-4DC6-B945-CB95B4233E3C}  Browser Typed URLs Setting Handler
{ADBE6DEC-9B04-4A3D-A09C-4BB38EF1351C}  XAML Browser Application
{ADC6CB82-424C-11D2-952A-00C04FA34F05}  Alpha
{ADC6CB86-424C-11D2-952A-00C04FA34F05}  DropShadow
{ADC6CB88-424C-11D2-952A-00C04FA34F05}  Wave
{ADD18BF7-AB60-4283-A580-D7544DD255D2}  AudioDeviceGraph Class
{add36aa8-751a-4579-a266-d66f5202ccbb}  Print Ordering via the Web
{ADE27590-4C84-4ABB-AE56-8233CC73D80F}  MrtStringResolver Class
{ADE6444B-C91F-4E37-92A4-5BB430A33340}  AppEventsDHTMLConnector 1.0 Object
{ADF2F380-ECE4-4969-91B8-FABA5681F2B9}  ConnectionManager Class
{ADF95821-DED7-11D2-ACBE-0080C75E246E}  Property Setter
{adfa80e7-9769-4ad9-992c-55dc57e1008c}  StartMenuAllPrograms
{AE03A0A5-DE98-45ff-8016-DDEFF70BCF61}  SAL File
{AE054212-3535-4430-83ED-D501AA6680E6}  Shell Name Space ListView
{AE0DB8A9-8183-4FA1-AFDA-C3506921D7E3}  Microsoft Account Child Info
{AE17FC35-F74E-45DB-9CCF-35193D4F7622}  Favorite Shortcuts Setting Handler
Callback
{AE1E00AA-3FD5-403C-8A27-2BBDC30CD0E1}  Home Networking NAT Traversal via UPnP
Configuration Manager
{ae2079d8-d764-4d79-ab4d-3543847a1a2c}
{AE24FDAE-03C6-11D1-8B76-0080C744F389}  Microsoft\Scriptlet Component
{ae4bbad2-f56a-4dfd-af17-79c03af451d0}  LauncherServiceHost
{ae5c828c-66a3-46e5-83f0-5ba1d7aa7752}
Windows.Networking.Sockets.ControlChannelTriggerEventDetails
{AE62C05D-0A02-30E7-9B51-E9D4DD157207}
{AE6BE008-07FB-400D-8BEB-337A64F7051F}  TF_TransitoryExtensionUIEntry
{AE6C819B-3A9B-4261-B4E5-14285EC46705}  CLSID_DialogManager
{AE8AFD54-5B57-4961-8A9B-12ADF23B696A}
{AE92E42B-4111-427A-8B0C-24A8D1A7D7F3}
{AE9472BF-B0C3-11D2-8D24-00A0C9441E20}  GrfCache Class
{AEB16279-B750-48f1-8586-97956060175A}  MF ASF Property Handler
{AEB84C83-95DC-11D0-B7FC-B61140119C4A}  DiskManagement.Control
{AEC17CE3-A514-11D1-AFA6-00AA0024D8B6}  DirectMusicSynthSink
{AED6483E-3304-11d2-86F1-006008B0E5D2}  Video Render Dynamic Terminal
{AED6483F-3304-11d2-86F1-006008B0E5D2}  Media Streaming Dynamic Terminal
{AEDAE7A2-E503-487B-8808-DF0BDDB5C422}  PSFactoryBuffer
{AEE2420F-D50E-405C-8784-363C582BF45A}  DevicePairingFolder Initialization
{AF02484C-A0A9-4669-9051-058AB12B9195}  File Save Dialog Legacy
{af076a15-2ece-4ad4-bb21-29f040e176d8}  EnhancedStorageACT Class
{af13dff0-e40f-4e6b-b4cd-009b81be6f6d}  IMEHistoryStoreConflictResolverJpn
{AF2440F6-8AFC-47d0-9A7F-396A0ACFB43D}  PSFactoryBuffer
{AF279B30-86EB-11D1-81BF-0000F87557DB}  Wipe
{AF2AC6EE-2B16-4756-9475-F319E543EFAA}  SOAPRequest Class
{AF44BF80-36DD-4118-B4CF-8B1E3F4FB9CE}  PSFactoryBuffer
{AF4B1274-B78A-4979-AEF5-20E78FEE102E}  MF AVI Sink Class Factory
{AF4F6510-F982-11d0-8595-00AA004CD6D8}  Registry Tree Options Utility
{af5c828c-66a3-35d4-9401-5ba1d7aa7752}
```

Page 92

```
                          SOFTWARE OUTPUT.txt
Windows.Networking.Vpn.Internal.VpnChannelEventDetails
    {AF604EFE-8897-11D1-B944-00A0C90312E1}  Microsoft Common Browser Architecture
    {AF65E2EA-3739-4e57-9C5F-7F43C949CE5E}  Copy-To Choose Folder
    {AF679D58-078E-48D4-A1E3-474F10DF76B8}  PSFactoryBuffer
    {AF75D6AD-E307-4052-8CB1-BF2052E734F0}  Windows.Data.Xml.ProxyStub
    {AF7FEAD8-C345-4600-8894-6D6F0E5EDDCD}  WiFi Connection APIs
    {AF95DC76-16B2-47F4-B3EA-3C31796693E7}
    {af9d2278-060f-4a17-99a9-5044f7f843a8}  CImeProperty_JK Class
    {AF9F2C0D-6B9F-4e32-A94D-A3E235A31BF7}  XML property store
    {AFA470FE-371D-4F98-9592-39E3C7227E5C}  State and invocation of verb commands
which are a list of commands
    {AFB40FFD-B609-40A3-9828-F88BBE11E4E3}  Server XML HTTP 3.0
    {AFB6C280-2C41-11D3-8A60-0000F81E0E4A}  MPEG-2 Demultiplexer
    {AFBA6B42-5692-48EA-8141-DC517DCF0EF1}  Server XML HTTP
    {AFC00D5E-BE1D-44A2-B875-7F7BDFAB1A18}  CM Policy CSP
    {afd198ac-5f30-4e89-a789-5ddf60a69366}  Bluetooth Radio Media Manager
    {AFD7F94B-1627-436c-80C8-B464AA21CAD3}  WMPlayer SecurityPropPage Class
    {AFEE8F8B-2FE6-4382-A0DE-8D713258B95E}  WindowsLicensing
    {AFFA1DA9-C637-4e6b-A0F3-276889D09F14}  Persist Peer XML
    {b020b123-89b9-46c6-8509-a8bf70447fea}  PSFactoryBuffer
    {B0210780-89CD-11d0-AF08-00A0C925CD16}  DirectSoundCapture Object
    {B021FF57-A928-459c-9D6C-14DED0C9BED2}  PrinterQueueView Class
    {B0271158-70D2-4C5B-9F94-76F549D90FDF}  MF AMRNB Media Sink
    {B02E0336-9E13-4E74-8A0A-7F04A273ADE8}  {B02E0336-9E13-4E74-8A0A-7F04A273ADE8}
    {B039282F-BE70-44BC-9862-966F4E95072F}  Family.Cache.ProxyStub
    {B0395DA5-6A15-4E44-9F36-9A9DC7A2F341}  MMC IconControl class
    {b03c2205-f02e-4d77-80df-e1747afdd39c}  ExecModelProxy
    {B03C7B74-40A6-4ED9-A900-A5873C15E8F1}  PSFactoryBuffer
    {b040ea9e-3f5e-48c9-bcdc-304e9d02851f}  CSdGITManager Class
    {B05DABD9-56E5-4FDC-AFA4-8A47E91F1C9C}  IVideoEncoderCodecAPIProxy
    {B07CAC5C-9786-4F8A-8DC7-902A6386F3E7}  SerialCapabilityHandler
    {B084785C-DDE0-4d30-8CA8-05A373E185BE}  NSC Byte Stream Handler
    {B091E540-83E3-11CF-A713-0020AFD79762}  File Types Page
    {B0A2AB46-F612-4469-BEC4-7AB038BC476C}  WMI High Performance Cooker
    {B0A8F3CF-4333-4bab-8873-1CCB1CADA48B}  Drive Type Categorizer
    {b0c43320-2315-44a2-b70a-0943a140a8ee}  XPS Signature Manager
    {B0D17FC2-7BC4-11d1-BDFA-00C04FA31009}  CLSID_IFontCache
    {B0DC057D-FA13-4CB3-B54D-4CC05E125781}
    {B0DDD260-9E44-4bf2-8602-6D9CE1D0B94F}  UCM Helper Class
    {B0EDF163-910A-11D2-B632-00C04F79498E}  MS TV Video Control
    {B0F1B174-AC86-452D-BAE7-C105F0F98C5A}  SecurityPolicyCSP
    {B115690A-EA02-48D5-A231-E3578D2FDF80}  CImeServerCht
    {B11CD547-573E-4D53-8719-D55634E3F458}  Accessibility Dock
    {b11d16d0-e195-4ca6-bbd5-1254ec098953}  6To4 Helper Class
    {B12AE898-D056-4378-A844-6D393FE37956}  Windows ThemeUI Pages
    {b1325ef5-dd4d-4988-a2b3-c776ad45d0d6}  Authentication UI Legacy Shutdown Dialog
    {B138E92F-F502-4adc-89D9-134C8E580409}  FileRecordingTerminal Class
    {b155bdf8-02f0-451e-9a26-ae317cfd7779}  delegate folder that appears in Computer
    {B15B8DC0-C7E1-11d0-8680-00AA00BDCB71}  SoftDist
    {B164BCEE-41B3-4F70-A53C-2ACA322DCCCB}  FhFileOperation Class
    {B1840AE4-5D39-4B8E-BEDD-82F251A5FF70}
    {B196B286-BAB4-101A-B69C-00AA00341D07}  PSFactoryBuffer
    {b1aebb5d-ead9-4476-b375-9c3ed9f32afc}  SppSvcRestartTaskHandler Class
    {B1AEC16F-2383-4852-B0E9-8F0B1DC66B4D}
    {B1B77C00-C3E4-11CF-AF79-00AA00B67A42}  DV Video Decoder
    {B1E29D59-A675-11D2-8302-00C04F8EE6C0}  SpGrammarCompiler Class
    {B1EBFC28-C9BD-47A2-8D33-B948769777A7}
    {B2B4135-168D-47D0-A6CE-78DAD1F2AA30}  OOBE RecommendedSettings Wizard Page
    {B20D5479-88CB-418e-A2F6-B4343B7680FE}  NarratorToolBar Class
    {B210D694-C8DF-490d-9576-9E20CDBC20BD}  Color Calibration Loader
    {b21858c6-9711-4257-99c8-5c0084bebce1}  DockInterface COM server
    {B22C3339-87F3-4059-A0C5-037AA9707EAF}
    {B2420E45-60BC-4466-AD5C-369EB092BEF8}  LegacyShareFlow
                            Page 93
```

SOFTWARE OUTPUT.txt

```
{B243A9FD-C57A-4D3E-A7CF-21CAED64CB5A}   CLSID_CoreUICoreWindowFactoryProxy
{B2445657-090D-11e4-AEDA-B4B52FE06611}   MTF Suggestion Client
{b27b520e-46db-4720-b9c5-5f80acab23a4}   HomeGroup Task
{b289af55-2833-44e0-a46f-96e5ebbd5c1b}   Refresh View Explorer Command
{b2952b16-0e07-4e5a-b993-58c52cb94cae}   CLSID_DBFolder
{B2A7FD52-301F-4348-B93A-638C6DE49229}   WMPSkinMngr Class
{b2b4fb61-d2dd-4ddd-8001-20f98c6577ef}   Microsoft Query Edit Control
{b2bcff59-a757-4b0b-a1bc-ea69981da69e}   AzAuthorizationStore Class
{b2cabfe4-fe04-42b1-a5df-08d483d4d100}   Windows Antimalware Scan Interface proxy
stub
{B2E8D89A-7A99-4b43-9638-DF4FF83EAC11}
{B2F2E083-84FE-4a7e-80C3-4B50D10D646E}   Default Category Provider
{B2F3A67C-29DA-4C78-8831-091ED509A475}   Microsoft Network Provider
{B2F586D4-5558-49D1-A07B-3249DBBB33C2}   DirectSoundBufferConfig Object
{B2F926DB-49FA-4958-914D-A260575403F7}   Visual Element DataLayer Helpers
{b3179149-2b99-48b2-b44b-11aa2034c1a3}   CCNGProvider
{B31C5FAE-961F-415b-BAF0-E697A5178B94}   IE Microsoft Multiple AutoComplete List
Container
{B323F8E0-2E68-11D0-90EA-00AA0060F86C}   StillImage
{B32D3949-ED98-4DBB-B347-17A144969BBA}   Sync Center Item Properties Extension
{B32F4002-BB27-45FF-AF4F-06631C1E8DAD}   PSFactoryBuffer
{B33F0D7A-1571-4022-B710-D26E9B87DEB8}   Autoplay Content Handler
{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC0}   @%systemroot%\system32\eqossnap.dll,-30001
{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC1}   @%systemroot%\system32\eqossnap.dll,-30001
{B35913A2-BE2E-4FA6-978C-3B130A7EFB98}   QuickActionsPS
{B359B02E-55E2-4B7D-B582-01089BAAA6AE}   XblGameSaveProxy
{B35EA47E-FA71-34FD-B7E2-EBC050A4FB5A}
{B37BF7D7-B78E-4465-98DE-71732453B03D}   HomeGroup Capabilities
{B3AADFEA-8404-4CBE-A62E-B0B715412C9E}   AppActivationFailedHandler
{B3E82D1C-E5A9-49a5-A189-2A38ACC1B2D7}   NarratorTable Class
{B3EE7802-8224-4787-A1EA-F0DE16DEABD3}   CheckerBoard
{B3FD5602-EB0F-415E-9F32-75DA391D6BF9}   ExecutivePlatform
{B3FE7F3F-B175-4159-A2DC-0F7F6606A878}   Clipboard Server
{B3FF88A4-96EC-4CC1-983F-72BE0EBB368B}   Rsop Logging Mode Provider
{B401C5EB-8457-427F-84EA-A4D2363364B0}   MSVidCtl FilePlayback to Video Renderer
Composition Segment
{B4124623-FC0E-47CE-BCA9-126A6104ADA1}   JournalReader Class
{B43A0C1E-B63F-4691-B68F-CD807A45DA01}   MSTSWebProxy Class
{B43C4EEC-8C32-4791-9102-508ADA5EE8E7}   IVideoEncoderProxy
{b4414d52-69c9-4666-b62a-d82620bed434}   Sort Groups Descending Explorer Command
{B44392DA-499B-446b-A4CB-005FEAD0E6D5}   MF Media Engine Class Factory
{b455f46e-e4af-4035-b0a4-cf18d2f6f28e}   Pin To Frequent Command
{B4601B57-1905-40E0-A33C-804B3AD24F2E}   DiagnosticLogCSP
{B474265E-3EF5-46E8-9FD9-AE034F34FC74}   wpnservice
{B488CB7E-98BC-4FA9-9FCA-E461728EFDCE}   PSFactoryBuffer
{B49FE003-49CC-4f36-BD61-9E6AE9C2175C}   TextSelectionChangedEvent Class
{B4A6821D-4D2E-40DD-9EE0-89C2CD07BF69}   Storage WMI Provider
{B4B3AECB-DFD6-11d1-9DAA-00805F85CFE3}
{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
{B4C8DF59-D16F-4042-80B7-3557A254B7C5}   Bluetooth PAN Profile Class Manager
{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}   Other Users Folder
{B5148095-4805-4DE7-986D-2456A0B7C838}   LayerManagerInproc Class
{B52D54BB-4818-4EB9-AA80-F9EACD371DF8}   Windows Search Platform
{B54E85D9-FE23-499F-8B88-6ACEA713752B}
{B54F3741-5B07-11cf-A4B0-00AA004A55E8}   VB Script Language
{B54F3742-5B07-11cf-A4B0-00AA004A55E8}   VB Script Language Authoring
{B54F3743-5B07-11cf-A4B0-00AA004A55E8}   VBScript Language Encoding
{B5607793-24AC-44c7-82E2-831726AA6CB7}   Free Space Categorizer
{b5827163-52b0-42c2-940f-f1d72cab1251}   WMPMDE NETCHANNEL ACTIVATE
{b5866878-bd99-11d0-b04b-00c04fd91550}   TypeFactory
{B58ED99D-A528-4E1B-A26C-0204D5A43718}   Accessiblity Setting Monitor
{B5965ACC-842D-4ABE-A618-9292BB3EE666}   MSASR Locale Handler Class (2052)
{B5A123C0-3893-4F1C-8599-00F4B82F2C99}   FhSearchProtocol Class
```

Page 94

SOFTWARE OUTPUT.txt

```
{b5a60a9e-a4c7-4a93-ac6e-0b76d1d87dc4}   Device Center Scan Context Menu Extension
{B5C8B898-0074-459F-B700-860D4651EA14}
{B5CFEB0E-9C01-4942-A5CB-F62EB09D808F}   Setting Sync Monitor Shell Service Object
{B5DF6DDB-8DEB-4984-961A-0E252214B016}   CLSID_MIMEReader
{B5EBAFB9-253E-4A72-A744-0762D2685683}
{b5f3bb7e-afaa-4b46-acbd-e12587329785}   StorageManager
{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}   MSAA AccPropServices
{B5F8FB3B-393F-4F7C-84CB-504924C2705A}   PSFactoryBuffer
{B60D6653-FDE4-4045-B5FD-F47B1BD45CA0}   WinRtTracing Proxy
{B6390DB1-4C44-4BA4-BA51-BBF4BED47C37}   XblAuthManagerProxyStubFactory
{B64016F3-C9A2-4066-96F0-BD9563314726}   BDA Tuning Model DVB-Satellite Tuning
Space
{B65449EC-4319-4C96-9ABD-E9257D00DB84}   Microsoft Network Adapter WMI Provider
{b66d6057-5f10-403c-87a5-88dae2813806}   Windows Push Notification Setting Handler
{b67c0b5e-c0ff-41c6-885d-5bdcd71837aa}   User State WMI Provider
{B6A585C5-804B-4837-8829-E43D85926DBF}   Notify backup restore status
{B6AFFB50-6F46-49B1-B912-C3F7A876CCCA}
{b6baabcf-8c41-4ccc-82e7-bc867662b833}   CMVCellular
{B6C292BC-7C88-41EE-8B54-8EC92617E599}   WIA Device Manager 2
{b6dc98b1-0bec-45e1-b2e4-3a2d943f0be4}   CDPAPIProvider
{B6FFEC3A-07F7-42D0-8829-B722F46DB533}   WinOpcIrmProtector Class
{B708457E-DB61-4C55-A92F-0D4B5E9B1224}   MMCViewExt 1.0 Object
{B7259EF0-83A6-4A3B-A2ED-93EE23DE7863}   DeviceAccessEvents
{B727ED66-3CF2-42fa-A5DA-C08121B33443}   NarratorListItem Class
{B72F8FD8-0FAB-4dd9-BDBF-245A6CE1485B}   QueryParser Class
{b7373566-8ff2-45d8-af1f-da39f289bcf9}   Folder Network Drive
{B744304E-083F-42d0-B969-A9F4EFC67610}   Provider Manager
{b75ac000-9bdd-11d0-852c-00c04fd8d503}   ADs Access Control Entry Object
{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}   ShellItemArray Shell Namespace helper
{B77C4C36-0154-4c52-AB49-FAA03837E47F}   CLSID_PublicationServicesServer
{B786ECB7-8942-4FE1-9DCD-230E30DE5AFF}   SpShortcut Class
{B79848C3-4F26-4D9D-BF1D-81FDF2704CF8}   OOBE Wireless Wizard Page
{B7AF5717-2927-469D-80D9-27873FB75FC3}   CLSID_MIMEBase64Decoder
{B7BBD408-F09C-4aa8-B65E-A00B8FE0F0B9}   Windows Theme Preview API
{B7BFFB5A-EFA8-4D8C-BBDE-C8D5FAAF54A1}   WOF Task Handler
{b7f5540c-5012-4acd-a4c6-b4b7efdcd851}   JumpViewExecuteHelperCF
{B8069D2E-4A49-475A-8FD2-533992303C2C}   CloudExperienceHost User Preffered Colors
Default Implementation
{B80AB0A0-7416-11D2-9EEB-006008039E37}   MJPEG Compressor
{B832674A-F36F-4780-AE4C-1566AAE3A4F4}   OOBE HidPairing Plugin
{B8445657-C149-4F95-8CFF-49D39B615F27}   MTF Suggestion List
{B8558612-DF5E-4F95-BB81-8E910B327FB2}   Sync Center (Private)
{b855b632-7dfb-4826-a172-3600ebd86948}   CImeDictAPILexiconBuilder Class
{b85ea052-9bdd-11d0-852c-00c04fd8d503}   ADs Access Control List Object
{B862BC49-E7E7-427E-868A-DE0F7A75BC07}   DMClient
{B87BEB7B-8D29-423F-AE4D-6582C10175AC}   Video Mixing Renderer
{B890AF56-AC8C-11D1-8CB7-00C04FC3261D}   CLBDTDispenser Class
{b8967f85-58ae-4f46-9fb2-5d7904798f4b}   Property System
{B8A27942-ADE7-4085-AA6E-4FADC7ADA1EF}   PNPX Pairing Handler Class
{B8B3F797-E237-4D1C-998A-1411D95B8C82}   RemoteFind
{B8BE1E19-B9E4-4ebb-B7F6-A8FE1B3871E0}   Microsoft Windows Font IExtractImage
Handler
{B8C54ECD-6BCE-4664-8DFD-016B751870D0}   NarratorIPOctet Class
{b8cdcb65-b1bf-4b42-9428-1dfdb7ee92af}   Compressed (zipped) Folder Context Menu
{b8f87e75-d1d5-446b-931c-3f61b97bca7a}
{b8fc52f5-cb03-4e10-8bcb-e3ec794c54a5}
{B8FD8075-9697-4699-BC64-0AAC0F76758E}   OOBE ProtectPC Settings Page 2
{B9033E87-33CF-4D77-BC9B-895AFBBA72E4}
{B9162A23-45F9-47CC-80F5-FE0FE9B9E1A2}   Bidi Spooler APIs
{b918dbc4-162c-43e5-85bf-19059a776e9e}   Remove From Frequent Places Command
{b91a4db4-3630-11dc-9eaa-00161718cf63}   Burn command invocation
{B91D5831-B1BD-4608-8198-D72E155020F7}
{B92E345D-F52D-41F3-B562-081BC772E3B9}
```

Page 95

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {B932D772-B787-4FBD-B82F-B2499A8269A4} | ModeManager Class |
| {b958f73c-9bdd-11d0-852c-00c04fd8d503} | ADs Security Descriptor Object |
| {B96F67A2-30C2-47E8-BD85-70A2C948B50F} | GradientWipe |
| {B977CB2D-EC6E-4A8F-BFFE-D18682BB0D52} | IShareMediaSettingsWriter |
| {b9815375-5d7f-4ce2-9245-c9d4da436930} | CLSID_PreviewEmail |
| {B98A2BEA-7D42-4558-8BD1-832F41BAC6FD} | Windows 7 File Recovery |
| {B9931692-A2B3-4FAB-BF33-9EC6F9FB96AC} | TF_LangBarItemMgr |
| {B9A160BE-0EB0-46A4-9942-30EB90BD792D} | Rude Window Manager |
| {B9B05098-3E30-483F-87F7-027CA78DA287} | Application Frame Host |
| {b9b61a03-caa7-43bb-b859-acd26d73b3f7} | CLSID_ResultHandlerFactory |
| {B9E84FFD-AD3C-40A4-B835-0882EBCBAAA8} | UPnPDevices Class |
| {B9F8535E-BF74-41C2-A6A6-7124442450DC} | CommandStore Action Dispatcher |
| {B9F8AC3E-0F71-11D2-B72C-00C04FB6BD3D} | Ks IBasicAudio Interface Handler |

Fri Jul 10 11:05:02 2015 Z

| | |
|---|---|
| {BA126AD1-2166-11D1-B1D0-00805FC1270E} | Network Connection Manager Class |
| {BA126AD2-2166-11D1-B1D0-00805FC1270E} | Network Connection Manager Connection Enumerator Class |
| {BA126AD3-2166-11D1-B1D0-00805FC1270E} | LAN Connection Manager Class |
| {BA126AD4-2166-11D1-B1D0-00805FC1270E} | LAN Connection Manager Connection Enumerator Class |
| {BA126AD5-2166-11D1-B1D0-00805FC1270E} | WAN Connection Manager Class |
| {BA126AD6-2166-11D1-B1D0-00805FC1270E} | WAN Connection Manager Connection Enumerator Class |
| {BA126AD7-2166-11D1-B1D0-00805FC1270E} | Dial-up Connection Class |
| {BA126AD8-2166-11D1-B1D0-00805FC1270E} | Network Group Policies for NLA Class |
| {BA126AD9-2166-11D1-B1D0-00805FC1270E} | Inbound Connection Class |
| {BA126ADB-2166-11D1-B1D0-00805FC1270E} | LAN Connection Class |
| {BA126ADD-2166-11D1-B1D0-00805FC1270E} | Inbound Connection Manager Class |
| {BA126ADE-2166-11D1-B1D0-00805FC1270E} | Inbound Connection Manager Connection Enumerator Class |
| {BA126ADF-2166-11D1-B1D0-00805FC1270E} | Network Install Queue |
| {BA126AE0-2166-11D1-B1D0-00805FC1270E} | Shared Access Connection Manager |
| {BA126AE1-2166-11D1-B1D0-00805FC1270E} | Shared Access Connection Manager Enumerated Connection |
| {BA126AE2-2166-11D1-B1D0-00805FC1270E} | Shared Access Connection |
| {BA126AE3-2166-11D1-B1D0-00805FC1270E} | Home Networking Connections Ultility Class |
| {BA126AE5-2166-11D1-B1D0-00805FC1270E} | Network Connection Manager Class 2 |
| {BA126E01-2166-11D1-B1D0-00805FC1270E} | Connection Manager LUA Inproc Object |
| {BA126F01-2166-11D1-B1D0-00805FC1270E} | Connection Manager LUA Host Object |
| {BA441419-0B3F-4FB6-A903-D16CC14CCA44} | CLSID_LockScreenContentionFlyout |
| {BA5BDA58-9D0A-47BB-93D1-6655AEDA6517} | Package State Conflict Resolver |
| {BA677074-762C-444b-94C8-8C83F93F6605} | User hive background upload task handler |
| {ba6ee7d8-190d-423a-93cc-1270e6599195} | |
| {ba6f127a-44ab-4674-b8f3-7131fa4dc645} | CLSID_SearchUriHandler |
| {BA7C0D29-81CA-4901-B450-634E20BB8C34} | CPrintTicket WoW Services |
| {ba818ce5-b55f-443f-ad39-2fe89be6191f} | Function Instance Collection Class |
| {BA9BB214-D930-4206-8F8F-BF0F1EAA4A6B} | PSFactoryBuffer |
| {BADCC35D-8542-4A5C-A457-0ECCCF62508A} | DSC Core |
| {BAE3E62C-37D4-49AC-A6F1-0E485ECD6757} | SREngine Class |
| {BAE86DDD-DC11-421C-B7AB-CC55D1D65C44} | PSFactoryBuffer |
| {BAEA8DC9-45F5-4DF8-A27F-2A277D524B15} | WIA Extension Host for 64 bit extensions |
| {baffdff4-240b-4c36-8173-70c8301d7753} | CloudExperienceHost Default Elevation Broker Context |
| {BB06C0E4-D293-4f75-8A90-CB05B6477EEE} | System |
| {BB07BACD-CD56-4E63-A8FF-CBF0355FB9F4} | EventSystem.EventObjectChange2 |
| {BB08E6F8-8877-4AC9-B224-E71D2ED5968F} | CPathItemExecuteCommand |
| {BB0D7187-3C44-11D2-BB98-3078302C2030} | CfgComp Class |
| {BB0DB60E-FFA0-4756-9F04-A0FCE6A97809} | PSFactoryBuffer |
| {BB18C7A0-2186-4be0-97D8-04847B628E02} | WpcProviderSupport Class |
| {BB2D41DF-7E34-4F06-8F51-007C9CAD36BE} | WlanAdhoc LUA |
| {BB2FEB41-0FF4-4BE9-A9A8-DAD0FAE602AA} | ChtQuickDS |
| {BB331DDE-CA08-4436-9C2F-4A84964703F4} | Windows.Storage.ApplicationData |
| {BB44391D-6ABD-422f-9E2E-385C9DFF51FC} | DxtCompositor Class |

Page 96

SOFTWARE OUTPUT.txt
```
{BB530C63-D9DF-4B49-9439-63453962E598}   Encoder Feature Segment
{BB64F8A7-BEE7-4E1A-AB8D-7D8273F7FDB6}   Security and Maintenance CPL
{bb6df56b-cace-11dc-9992-0019b93a3a84}   Background Intelligent Transfer Control
Class 4.0
{BB847B8A-054A-11d2-A894-0000F8084F96}   CLSID_IPropFindRequest
{BB89EB37-081E-4F5D-BA35-8D636BB47440}   MSASR Locale Handler Class (1028)
{BB918E32-2A5C-4986-AB40-1686A034390A}   Plug-in Terminal Class
{bbb5d0e2-6f4b-4c31-8744-22d0029c4b40}   Function Discovery Print Provider
{BBB9389D-CB46-4855-ADA6-4570E7342B3C}   Ribbon Share With Verb
{BBC035D1-E5A1-44F5-A166-E70DAED1CB02}
{BBC29D47-09E4-453E-9A08-B0AE77CAD120}   ApplicationTriggerDetails
{BBC40082-8ABB-4DDD-B1C6-4EE0A9A5DB52}   WMPlayer PlaylistPropPage Class
{BBCD9053-4392-41cf-BA00-5CB5DA2CEF71}   ArgDictionary Class
{BBD5AFE4-1417-40f7-94B3-A10719535CB4}   FhCatalog Class
{BBD8C065-5E6C-4e88-BFD7-BE3E6D1C063B}   Virtual Factory for Power Options Control
Panel
{BBEC4F81-C2BC-43a7-BD95-9738EE9B6CCA}   WMPlayer DVDPropPage Class
{bbeea841-0a63-4f52-a7ab-a9b3a84ed38a}   MP3 Decoder DMO
{BC065925-E8EF-4EF7-B8C5-006C8DB832D5}   SpMMAudioOut Class
{BC08386A-9952-40CD-BA50-9541D64A4B4E}   PSFactoryBuffer
{bc13e0f8-164a-47f9-ae4b-21947643a06e}   CProvisioningCSP
{BC271022-28CD-468A-BBB0-EF7091D8625E}   Connecting Progress Page Class
{bc47fcfe-98a0-4f27-bb07-698af24f2b38}
{BC48B32F-5910-47F5-8570-5074A8A5636A}   Sync Results Delegate Folder
{bc65fb43-1958-4349-971a-210290480130}   Ncd Property Page
{BC94D813-4D7F-11d2-A8C9-00AA00A71DCA}   SdoService Class
{BCC9FF78-A268-4907-97AB-109C5C62C45B}
Windows.Devices.Bluetooth.Background.BluetoothLEAdvertisementWatcherTriggerDetails
{BCDE0395-E52F-467C-8E3D-C4579291692E}   MMDeviceEnumerator class
{bce9c4d2-0bd2-4ff7-8f94-d69225bb2c7f}   Background activation of raw notifications
{BCEA735B-4DAC-4B71-9C47-1D560AFD2A9B}   DfsShellAdmin Class
{BCED617B-EC03-420b-8508-977DC7A686BD}   WSMan Automation Class
{BD0D38E4-74C8-4904-9B5A-269F8E9994E9}   ImageProcess Class
{BD24FF86-6723-47B6-9C73-DA362CA6418F}   BackgroundMediaPolicy
{BD254A13-FAA8-42A1-8132-42D9E8B320DD}
{bd3739e8-3cf5-45fb-9cc3-28163c2e9ffd}
{BD472F60-27FA-11cf-B8B4-444553540000}   Compressed (zipped) Folder Right Drag
Handler
{BD4F77B3-70B0-4464-83A5-785F205B823B}   InkTablet Class
{BD5EB95F-1F8A-4D34-8F1E-C90BC772E64E}
{bd69ecaa-ae5c-40d0-b968-7848f3778f56}   DHCP Module Helper Class
{BD6EDFCA-2890-482F-B233-8D7339A1CF8D}
{BD70C020-2D24-11D0-9110-00004C752752}
{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}   @%systemroot%\system32\mssvp.dll,-112
{BD7BDFFF-FCF5-439C-ABE7-01D244849BFB}   NarratorElementFactory Class
{BD84B380-8CA2-1069-AB1D-08000948F534}   Microsoft Windows Font Folder
{BD84B381-8CA2-1069-AB1D-08000948F534}   PANOSE Core Mapper
{BD95BA60-2E26-AAD1-AD99-00AA00B8E05A}   SDSnapin Class
{BD96C556-65A3-11D0-983A-00C04FC29E33}   RDS.DataControl
{BD96C556-65A3-11D0-983A-00C04FC29E36}   RDS.DataSpace
{BD9C9B8F-0403-49D5-8AC2-2354385DF5E5}   TaskSchedulerUtil
{BDCD51FB-55A0-4486-908C-5240F23698AC}   Accessible Keyboard UI Class
{bde9ee7c-329f-4fcf-ba7a-f8c6e9b4579d}   DUI Shell View Frame
{BDF23680-C1E5-11D2-9EF7-006008039E37}   Pin Property
{BDFEE05A-4418-11DD-90ED-001C257CCFF1}   Mbn ConnectionProfile Manager
{BDFEE05B-4418-11DD-90ED-001C257CCFF1}   Mbn Interface Manager
{BDFEE05C-4418-11DD-90ED-001C257CCFF1}   Mbn Connection Manager
{BE09F473-7FEB-11d2-9962-00C04FA309D4}   CLSID_MigrateMessageStore
{BE0A9830-2B8B-11D1-A949-0060181EBBAD}   WMI MSI Provider
{be382474-a1dd-4dc9-aa9b-2a934d67bd10}   Icon Size Explorer Command
{BE5C1432-6A36-47c6-9C07-9BF8ED15B9C1}   NarratorTabItem Class
{be88f957-42cc-4da7-92cf-9bc35c5d5ee2}   CStorageFileProxy
{BE8E0170-72DC-11D2-952A-0060081840BC}   Stretch Property Page
```
Page 97

SOFTWARE OUTPUT.txt
```
{beb5488b-9954-402d-89df-1aedfe18ca1c}
Windows.Devices.Enumeration.DeviceWatcherTriggerDetails
    {BEB579D7-29C7-43B2-8D9C-53FC410AE9F3}    MCCS HeartBeatController
    {BEC09223-B018-416D-A0AC-523971B639F5}    WinBio Credential Provider
    {BED4D415-7971-4310-AA07-6AC15EA06ACC}    WinInet Helper Class
    {BEDAA0DF-7127-402D-9617-B26DB4AF2382}    DIALMetadataProvider Class
    {BEF723E2-01AD-438B-A441-D0112DF5142A}    Structured State Handler .
    {BF0AC53F-D51C-419F-92E3-2298E125F004}    Open Powershell as Admin Command
    {BF426F7E-7A5E-44D6-830C-A390EA9462A3}    DocWrap Class
    {bf50b68e-29b8-4386-ae9c-9734d5117cd5}    IShellFolder marshaler app compat stub
    {BF583E12-3C8B-4767-B732-CC8B34D1D65F}    TouchMonitor Class
    {bf5c828c-66a3-35d4-9401-5ba1d7aa7752}
Windows.Networking.Vpn.Internal.VpnChannelRtcEventDetails
    {BF5CB148-7C77-4d8a-A53E-D81C70CF743C}    AD RMS Rights Policy Template Management
(Manual) Task Handler
    {bf641d1c-29fd-4721-b3b8-48d92d35f7df}    CLSID_QueryFactoryWithOptions
    {bf75430d-51dd-483f-bc3a-4542e6c9dce4}    ShareFlow Class Factory
    {BF77196E-24EF-4A02-BD52-A626D7AE837E}    Browser History Setting Handler
    {BF782CC9-5A52-4A17-806C-2A894FFEEAC5}    Language Settings
    {bf78a650-d489-4360-a0b7-c32471e07692}    XML Filter Handler
    {BF85540E-0DF3-47bc-AC5D-305442704708}
    {BF87B6E0-8C27-11D0-B3F0-00AA003761C5}    Capture Graph Builder
    {BF87B6E1-8C27-11D0-B3F0-00AA003761C5}    Capture Graph Builder 2
    {BF8841C9-378A-4CAD-B4FC-5091366CBC0D}    Shell AutoPlay Direct
    {BF981FDD-B743-11D1-A69A-00C04FB9988E}    MachineSettings Class
    {BFAD62EE-9D54-4b2a-BF3B-76F90697BD2A}    IE Shell Rebar BandSite
    {BFC7DC7B-8F11-4A40-8DB2-207302E2D61B}    PSFactoryBuffer
    {BFC880F1-7484-11d0-8309-00AA00B6015C}    Download Site Manager
    {BFCD4A0C-06B6-4384-B768-0DAA792C380E}    UIAnimationTimer
    {BFD468D2-D0A0-4bdc-878C-E69C2F5B435D}    CLSID_PreviewUrl
    {BFD6E7B9-2FDE-413E-9AC9-52FC8656908C}
    {BFE18E9C-6D87-4450-B37C-E02F0B373803}    AutomaticUpdates
    {BFFECCA7-4069-49F9-B5AB-7CCBB078ED91}
System.ServiceModel.Internal.TransactionBridge
    {c00d8ee5-7325-49b5-b83d-e4f42ba7e073}    QuickLinks Setting Handler
    {C03E8500-781E-49a1-8190-CE902D0B2CE7}    Connection to work options Page
    {C03E8511-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup CTI Hook Page (non-UI)
    {C03E8512-781E-49a1-8190-CE902D0B2CE7}    Dialup CTI Connection Retry Page
    {C03E8513-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup Connection Info Page
    {C03E8521-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup CTW Hook Page (non-UI)
    {C03E8522-781E-49a1-8190-CE902D0B2CE7}    Dialup CTW Connection Retry Page
    {C03E8523-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup (CTW) Connection Info Page
    {C03E8524-781E-49a1-8190-CE902D0B2CE7}    RAS Dialup (CTW) User Info Page
    {C03E8531-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Check Internet Connection
    {C03E8532-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Hook Page (non-UI)
    {C03E8533-781E-49a1-8190-CE902D0B2CE7}    RAS VPN Connection Info Page
    {C03E8534-781E-49a1-8190-CE902D0B2CE7}    RAS VPN User Info Page
    {C03E8541-781E-49a1-8190-CE902D0B2CE7}    RAS PPPoE Hook Page (non-UI)
    {C03E8542-781E-49a1-8190-CE902D0B2CE7}    RAS PPPoE Connection Info Page
    {C03E8551-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Check Devices Page
    {C03E8552-781E-49a1-8190-CE902D0B2CE7}    RAS Incoming Connection Hook Page (non-UI)
    {C03E8553-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Users Page
    {C03E8554-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Devices Page
    {C03E8555-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Network Page
    {C03E8556-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Save Page
    {C03E8557-781E-49a1-8190-CE902D0B2CE7}    Incoming Connection Summary Page
    {C03E8561-781E-49a1-8190-CE902D0B2CE7}    RAS New Connections Page
    {C03E8565-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Work Testing Page Class
    {C03E8566-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Internet Testing Page
Class
    {C03E8568-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Work Finish Page Class
    {C03E8569-781E-49a1-8190-CE902D0B2CE7}    RAS Connection To Internet Finish Page
Class
```

Page 98

SOFTWARE OUTPUT.txt

```
{C03E8571-781E-49a1-8190-CE902D0B2CE7}   VANUI RAS Connect Page Class
{C03E8572-781E-49a1-8190-CE902D0B2CE7}   VANUI RAS Disconnect Page Class
{C03E8581-781E-49a1-8190-CE902D0B2CE7}   Set up a new connection
{C03E8582-781E-49a1-8190-CE902D0B2CE7}   Set up a new virtual network connection
(VPN)
{C03E8583-781E-49a1-8190-CE902D0B2CE7}   Set up a new dialup connection
{C03E8584-781E-49a1-8190-CE902D0B2CE7}   Set up a new dialup connection (Internet)
{C03E8585-781E-49a1-8190-CE902D0B2CE7}   Broadband connection task class
{C03E8586-781E-49a1-8190-CE902D0B2CE7}   Incoming Connections Task Class
{C03E8588-781E-49a1-8190-CE902D0B2CE7}   Pre-CFE Page Class
{C03E8591-781E-49A1-8190-CE902D0B2CE7}   XWizard Factory Generated Class
{C03E8592-781E-49A1-8190-CE902D0B2CE7}   XWizard Factory Generated Class
{c047c5a9-c407-4a1e-ad7f-11d0861344b7}   L2Sec Helper Class
{C04D65CF-B70D-11D0-B188-00AA0038C969}   Multi Language String
{c08afd90-f2a1-11d1-8455-00a0c91f3880}   ShellBrowserWindow
{C0932C62-38E5-11d0-97AB-00C04FC2AD98}   SQLOLEDB Error Lookup
{c0aa878e-97a5-44df-b7ef-2e732f7b2fec}   TC IME Handwriting Applet
{C0AA9D93-2EF5-47FB-960C-F90FC644B48E}   Win32_JobObjectIOAccountingInfo Component
{C0AB2A0D-F2D2-46E2-9DF9-8885A424C29A}   File System Setting Handler2
{C0B19DEF-9E2A-48cd-B438-26663E22B025}   User Tile Flyout
{C0B35746-EBF5-11D8-BBE9-505054503030}   PSFactoryBuffer
{C0B3C446-3032-4016-926F-9BAE48BEBFBE}   IMOfferRA Class
{C0B4E2F3-BA21-4773-8DBA-335EC946EB8B}   File Save Dialog
{c0b9675c-a5e1-408c-b5df-f3bba520827c}   PSFactoryBuffer
{C0BC4B4A-A406-4EFC-932F-B8546B8100CC}   UPnPServices Class
{C0CD7D12-31FC-4BBC-B363-7322EE3E1879}   Microsoft ALAC Audio Decoder MFT
{C0DCC3A6-BE26-4bad-9833-61DFACE1A8DB}   Network Center LUA
{C0E13E61-0CC6-11d1-BBB6-0060978B2AE6}   Data Driven Cleaner
{C0E2E55A-5222-4810-BEA0-6AEF8092A000}   Package State Setting Monitor
{C100BE9A-D33A-4a4b-BF23-BBEF4663D017}   WCN Discovery Provider Class
{C100BEA3-D33A-4a4b-BF23-BBEF4663D017}   WCN Discovery Object
{C100BEBB-D33A-4a4b-BF23-BBEF4663D017}   WCN Elevation Helper
{C10B4771-4DA0-11D2-A2F5-00C04F86FB7D}   Winmgmt MOF Compiler
{C10E23A2-BFF0-4113-BCE8-C91BE754E281}   MF FLAC Media Property Handler
{C120DE80-FDE4-49f5-A713-E902EF062B8A}   MF MP3 Property Handler
{c1243ca0-bf96-11cd-b579-08002b30bfeb}   Plain Text filter
{C1282A7B-9455-48dc-BBBB-46C2EB525AF5}   WMPlayer VizResolutionPropPage Class
{c12a0aa6-acf8-4947-acf3-81bdce609353}   Windows.Devices.Background Proxy
{C12EC999-9D91-425E-84AF-DC15443A6B81}   OOBE End Wizard Page
{C1373050-E8C9-4AE4-A0C5-1DCF07274587}
{C139C040-532D-451b-80CA-44D1F0839D2A}   Share With Nobody
{c153e702-afcc-4f45-9a75-a70217f72db8}
{c15e6bf0-6351-4588-ac4f-ef7d5ec8c16e}   WMPlayer LibraryPropPage Class
{C17CABB2-D4A3-47D7-A557-339B2EFBD4F1}
{C185ECE5-0720-472c-B407-9BB4E8DD5E72}   Lock Screen Store
{C196B2BE-BA06-4049-8518-322E1E04282B}   ConfigManager2MutableURI
{C19FBD0E-7663-44ea-8265-74130671A1D6}   OpenSearch Description Location Creator
{C1E565E2-F2DE-4537-9612-2F30A160EB5C}   FaceDetectionMFT
{C1EE01F2-B3B6-4A6A-9DDD-E988C088EC82}   CActiveIMMAppEx
{C1F400A0-3F08-11D3-9F0B-006008039E37}   Sample Grabber
{C1F400A4-3F08-11D3-9F0B-006008039E37}   Null Renderer
{c1f85ef8-bcc2-4606-bb39-70c523715eb3}   ScheduledDiagnosticCustomHandler
{C20447FC-EC60-475E-813F-D2B0A6DECEFE}   Extensible Eventing Service
{c206f324-bb45-4765-93ff-3bca7306ff2e}   CommonLayoutDefinition
{C20CE506-5DA9-4B9C-9662-D88BD30E10A1}   PrinterQueueViewJobExtension Class
{C20ED5C4-0A2E-4F66-9BE2-86A1C823DD68}   PSFactoryBuffer
{C21B45B8-5D76-4575-BA27-54823098C491}   IE Microsoft Docking Bar Property Bag
{C22020C6-EEAB-455E-BEC2-A2CC8FDFF976}   OOBE ZDP Plugin
{C23FC28D-C55F-4720-8B32-91F73C2BD5D1}   SpPhraseInfoBuilder Class
{c2409f61-9d38-48a4-995f-1cfdb390b1d9}   Windows Insider Hub Broker
{c2467d33-71c5-4057-977c-e847c2286882}   By value marshaled confirmation interrupt
{C2566514-DD44-4c6c-AAAD-FBD2F18D8DEE}   Property Set Storage In Memory Object
{C2745EC3-CF23-4601-92EF-D189B711F933}
```

Page 99

SOFTWARE OUTPUT.txt

CAppointmentsProviderInternalChooseCalendarForViewActivationPlugin
```
{C274CC5B-44A9-4093-A686-71F88079C450}
{c278aba7-cc1c-4717-bdfb-db2bca78246e}    Grouping Helper Class
{C2796011-81BA-4148-8FCA-C6643245113F}    Network Tray SSO
{c27f6b1d-fe0b-45e4-9257-38799fa69bc8}    UsbCeip
{C2B136E2-D50E-405C-8784-363C582BF43E}    DeviceCenter Initialization
{c2b94e6d-6ebd-44ee-aac1-eb809c984699}    SeamlessAudio mft
{C2CF3110-460E-4fc1-B9D0-8A1C0C9CC4BD}    Desktop Wallpaper
{c2d2c3a4-9a7e-11da-8bf7-0007e95ead8d}    SBF File
{C2EA74E0-0ED2-11CF-A9BB-00AA004AE837}    Doc Object View
{c2f03a33-21f5-47fa-b4bb-156362a2f239}    Immersive Shell
{C2FBB630-2971-11d1-A18C-00C04FD75D13}    Microsoft CopyTo Service
{C2FBB631-2971-11d1-A18C-00C04FD75D13}    Microsoft MoveTo Service
{C2FEEEAC-CFCD-11D1-8B05-00600806D9B6}    Wbem Scripting Last Error
{C3203275-7A13-425F-8F7E-828C2D750337}
{c3278e90-bea7-11cd-b579-08002b30bfeb}    Null filter
{c350f6ad-f45f-45c9-9e62-1f50bb3fc25f}    Folder Redirection WMI Provider
{C3701884-B39B-11D1-9D68-00C04FC30DF6}    OleInstall Class
{c39ee728-d419-4bd4-a3ef-eda059dbd935}    WinInetBroker Class
{C39FF590-56A6-4253-B66B-4119656D91B4}    Exchange Active Sync Policies Broker
{C3A43F75-FE02-47d8-B3EE-0B568C0C5043}
{C3BDF740-0B58-11d2-A484-00C04F8EFB69}    CrBarn
{C3C39131-B182-4801-B437-6D1E65B72F57}    Shell User Accounts
{C3E5D3D2-1A03-11CF-942D-008029004347}    System Monitor General Properties
{C3E5D3D3-1A03-11CF-942D-008029004347}    System Monitor Graph Properties
{C4050BC4-29E1-4c8f-BF6E-6EBAD21E0673}    HomeGroup Printer Monitor
{C40D66A0-E90C-46C6-AA3B-473E38C72BF2}    Folder Redirection Editor
{C40FBD00-88B9-11d2-84AD-00C04FA31A86}
{C424F25A-6774-48BC-9F1E-02CCA8C1BE62}    Troubleshooting Control Panel
{C4270827-4F39-45DF-9288-12FF6B85A921}    EditionUpgradeBroker
{C437AB2E-865B-321D-BA15-0C8EC4CA119B}
```
System.Runtime.CompilerServices.NativeCppClassAttribute
```
{C439A42A-583F-4609-8C30-E3681E2A0E78}    Shell Namespace Setting Change Publisher
{C45268A2-FA81-4E19-B1E3-72EDBD60AEDA}    MSVidCtl Enhanced Video Renderer(DX10)
```
Segment
```
{c463a0fc-794f-4fdf-9201-01938ceacafa}    RasMobilityManager
{C47195EC-CD7A-11D1-8EA3-00C04F9900D7}    SysColorCtrl class
{c472004d-44fb-41e9-ac0a-7b920384a850}    Device Center Print Commands Extension
{C47A41B7-B729-424f-9AF9-5CB3934F2DFA}    WinSAT Query OEM Customization Object
{C4819C8D-9AB8-4B2F-B8AE-C77DABF553D5}    Microsoft WBEM Current Time Provider
{C49E32C6-BC8B-11d2-85D4-00105A1F8304}    Windows Management Instrumentation Backup
```
and Recovery
```
{c4bbedb4-e9b9-4e41-8fe1-0786480a2173}    CL2TPDiagHelper Object
{C4BF2784-AE00-41BA-9828-9C953BD3C54A}    MSVidCtl CC to Video Renderer Composition
```
Segment
```
{C4C4C481-0049-4E2B-98FB-9537F6CE516D}    Encrypt
{C4C4C482-0049-4E2B-98FB-9537F6CE516D}    Decrypt
{C4C4C483-0049-4E2B-98FB-9537F6CE516D}    Properties
{C4C4C491-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C492-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C493-0049-4E2B-98FB-9537F6CE516D}    Tags
{C4C4C4F1-0049-4E2B-98FB-9537F6CE516D}    Encrypt/Tag
{C4C4C4F2-0049-4E2B-98FB-9537F6CE516D}    Decrypt/Tag
{C4C4C4F3-0049-4E2B-98FB-9537F6CE516D}    XDS Codec
{C4D2D8E0-D1DD-11CE-940F-008029004347}    System Monitor Control
{C4D81942-0607-11D2-A392-00E0291F3959}    Big Switch
{C4D81943-0607-11D2-A392-00E0291F3959}    Smart Recompressor
{C4EC38BD-4E9E-4b5e-935A-D1BFF237D980}    Explorer Travel Band
{c51b83e5-9edd-4250-b45a-da672ee3c70e}    Restore Default Libraries Command
{C529C7EF-A3AF-45F2-8A47-767B33AA5CC0}    Network Diagnostics Framework
{C52FF1FD-EB6C-42CF-9140-83DEFECA7E29}    InkObjectXP Class
{C531D9FD-9685-4028-8B68-6E1232079F1E}    BDA Tuning Model DVB Cable Locator
{C5388469-F816-40D2-9E6B-D6C68986996E}
```
Page 100

SOFTWARE OUTPUT.txt

```
{c53e07ec-25f3-4093-aa39-fc67ea22e99d}  PSFactoryBuffer
{C555438B-3C23-4769-A71F-B6D3D9B6053A}  Display
{C5599E1B-FC7B-4883-9FF4-581BBAEF8DBA}  Bluetooth FD Provider Proxy
{C5702CCC-9B79-11D3-B654-00C04F79498E}  Input Devices Collection Class
{C5702CCD-9B79-11D3-B654-00C04F79498E}  Output Devices Collection Class
{C5702CCE-9B79-11D3-B654-00C04F79498E}  Video Renderers Collection Class
{C5702CCF-9B79-11D3-B654-00C04F79498E}  Audio Renderers Collection Class
{C5702CD0-9B79-11D3-B654-00C04F79498E}  Features Collection Class
{C5702CD6-9B79-11D3-B654-00C04F79498E}  Custom Composition Segment from Legacy
Analog Tv Tuner Device Segment to Data Services Feature Segment
{C578375F-8441-4733-BF71-027683AF538B}  Application Tile Information
{c57a6066-66a3-4d91-9eb9-41532179f0a5}  AppSuggestedLocations
{c585dc93-540e-4f56-b0dc-69f58f813e04}  PnpObjectServer
{c5872cfd-52d1-4494-aa0d-22d42bbb2e30}  Remove From Recent Documents Command
{C58BD103-E87F-4B78-A0FA-7A5C95970EE2}  AudioRateConvert Class
{C58C4893-3BE0-4B45-ABB5-A63E4B8C8651}  Troubleshooting
{c58ca859-80bc-48df-8f06-ffa94a405bff}  Picker Host
{C591F150-4106-4141-B5C1-30B2101453BD}  MF MKV Property Handler
{C5B19592-145E-11d3-9F04-006008039E37}  DxtKey Class
{C5B454CD-3CA1-4b3a-A1D0-2CB5CD6BD985}  Application Targeting Tracker
{C5C5C5F0-3ABC-11D6-B25B-00C04FA0C026}  XDSToRat Class
{C5C5C5F1-3ABC-11D6-B25B-00C04FA0C026}  EvalRat Class
{C5E2E36E-0D2D-4FAC-A9F4-DDAD14633222}  Microsoft Windows Net Event Capture WMI
Provider
{c5efd803-50f8-43cd-9ab8-aafc1394c9e0}  IE OpenService Activity Manager
{C605507B-9613-4756-9C07-E0D74321CB1E}  CLSID_HomeGroupCtrl
{C608E099-892D-4628-B6A2-97257B014E2E}
{C60F637A-07F3-411D-B577-22E519F8B63B}  ResourceManagerQueue Class
{C61BFCDF-2E0F-4AAD-A8D7-E06BAFEBCDFE}
{C624BA95-FBCB-4409-8C03-8CCEEC533EF1}  UPnPService Class
{C63261E4-6052-41FF-B919-496FECF4C4E5}  EntAppSvc
{c63382be-7933-48d0-9ac8-85fb46be2fdd}  Default Folder Menu
{C6365470-F667-11d1-9067-00C04FD9189D}  Gradient DXSurface
{C64501F6-E6E6-451f-A150-25D0839BC510}  Microsoft TTS Desktop Engine Class
{C647B5C0-157C-11D0-BD23-00A0C911CE86}  AVI mux Property Page
{C64B9B66-E53D-4c56-B9AE-FEDE4EE95DB1}  Condition History Class
{c658e5bd-817b-41c8-8fb6-5b2b386a40ea}
{C666E115-BB62-4027-A113-82D643FE2D99}  MPEG-2 Sections and Tables
{C68411EA-1396-48f3-AF98-B7F657E35C20}  Autoplay Device Handler
{c6887882-a444-4b32-960d-e40d0af7851e}  CLSID_FileInUsePLMResolver
{C6A4CF44-5069-4CD0-BD40-4437E4BE57EC}  NarratorInvokePattern Class
{C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7}  BDA Tuning Model DVB Tuning Space
{C6B167EA-DB3E-4659-BADC-D1CCC00EFE9C}  FodHelperComObject Class
{C6B400E2-20A7-4E58-A2FE-24619682CE6C}  Microsoft AC3 Encoder
{C6B5F214-0743-3868-B1EA-C4C23CE2AF52}
{c6cc0d21-895d-49cc-98f1-d208cd71e047}  Internet Explorer Settings Broker
{C6CC49B0-CE17-11D0-8833-00A0C903B83C}  CertGetConfig Class
{C6FABB24-E332-46FB-BC91-FF331B2D51F0}  SpPhoneConverter Class
{C6FCE351-A02B-466A-9235-D03134892D25}  Browser History File System Monitor
Callback
{C707F6A6-A1F3-45d7-99AA-A2B9491E84AD}  CLSID_PublicationServices
{C70D0E90-6FF8-40CC-B679-6CCFF0B2E673}  InkRectangle Class
{C71566F2-561E-11D1-AD87-00C04FD8FDFF}  Microsoft WBEM Universal Refresher
{c71c41f1-ddad-42dc-a8fc-f5bfc61df957}  Immersive Shell Builder
{C71C7533-AAA8-4315-9457-08DE2F558972}  CLSID_SMIME
{C72BE2EC-8E90-452c-B29A-AB8FF1C071FC}  FunctionDiscovery Class
{c73f6f30-97a0-4ad1-a08f-540d4e9bc7b9}  CLSID_AutoListPropertyStore
{C7657C4A-9F68-40fa-A4DF-96BC08EB3551}  Photo Thumbnail Provider
{c77a3c40-03fd-47f9-a279-356b38f36e26}  CSystemHandler
{C79A574C-63BE-44b9-801F-283F87F898BE}  SpWaveFormatEX Class
{c79d1575-b8c6-4862-a284-788836518b97}  Windows Display Settings
{c79f8f33-e5dc-4b89-8ea9-51dd1f5828f2}  DA OTP Credential Provider
{C7A3A54B-0250-11D3-9CD1-00105A1F4801}  Microsoft WBEM SMTP Event Consumer
```

Page 101

SOFTWARE OUTPUT.txt

```
Provider
   {C7BCD216-4A04-4EF4-A9EE-21EFD6948C9B}   CredentialSerialization
   {C7CA6167-2F46-4C4C-98B2-C92591368971}   New Library Menu Handler
   {C7D83DDF-EAD2-4536-86F5-6E88B89213AC}   Clipboard Notification Client
   {C7F2FB0F-ACC2-4ddf-9D8A-5E6E80D61024}   Search Filter Kind Command
   {C8059EB6-D2FC-4ecf-A15F-AF427F5E4DB6}   Feeds Background Sync
   {c82192ee-6cb5-4bc0-9ef0-fb818773790a}   JumpViewExecuteHelper
   {c827f149-55c1-4d28-935e-57e47caed973}   Shell Web Wizard Host Object
   {c8367320-6f85-11e0-a1f0-0800200c9a66}   BthTelemetry
   {C86D6E59-E9E6-489B-A6C3-37ED73ADBF5A}
   {C87CCFB7-8D32-45B8-A532-FFA533F44150}   GestureArbitrationEngine Class
   {C885AA15-1764-4293-B82A-0586ADD46B35}   IrisCredentialProvider
   {C89AC250-E18A-4FC7-ABD5-B8897B6A78A5}
System.EnterpriseServices.RegistrationHelperTx
   {c89e334c-e65f-4156-842e-ea89cec71dea}   WFP and IPsec Helper Class
   {C89FC3EF-A0DC-4feb-BFBC-F13A9C334D4F}   LockScreen Application Notification Broker
   {C8A1FAD9-BC51-4031-A3CB-00EDB3FD7D63}   OOBE OEM Registration Page
   {c8b522cc-5cf3-11ce-ade5-00aa0044773d}   MSDASQL ErrorLookup
   {c8b522cd-5cf3-11ce-ade5-00aa0044773d}   MSDASQL Enumerator
   {C8B522CF-5CF3-11CE-ADE5-00AA0044773D}   Microsoft OLE DB Error Collection Service
   {c8b522d0-5cf3-11ce-ade5-00aa0044773d}   Microsoft OLE DB Root Enumerator
   {c8b522d1-5cf3-11ce-ade5-00aa0044773d}   Microsoft OLE DB Data Conversion Library
   {c8c97725-c948-4720-bf0f-e3c2273bfb7d}   Library Initialization Handler
   {c8e6f269-b90a-4053-a3be-499afcec98c4}   User Account Control Check Provider
   {C8F19C79-F2F9-452B-A34E-8926333A4C7F}   ContinuousReadingRetryParameter Class
   {C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6}   PSFactoryBuffer
   {C907F3EA-0EB4-40BD-AAC0-D3D8C32B1840}   LayoutInvalidatedEvent Class
   {C90FB8CA-3295-4462-A721-2935E83694BA}   CLSID_SearchCommand
   {c9298eef-69dd-4cdd-b153-bdbc38486781}   State of verb Empty Recycle Bin
   {C947D50F-378E-4FF6-8835-FCB50305244D}   SyncInfrastructure Class
   {C96401CC-0E17-11D3-885B-00C04F72C717}   Folder
   {C96401CF-0E17-11D3-885B-00C04F72C717}   OCX
   {C96401D1-0E17-11D3-885B-00C04F72C717}   HTML
   {C96C4A08-12E9-4f87-8E6C-3DCF98518E11}   OOBE Language Plugin
   {C97AC1B3-8698-4BF6-8DBB-60F6064FA320}   PSFactoryBuffer
   {C985DF59-A91B-446B-93C3-FB2705D529BC}   CLSID_ImmersiveSplashScreen
   {C98F3822-3658-4D75-8A25-6621665ECD56}   HomeGroup Password Command
   {c99217e2-951d-40b6-b4e4-6af203dadf89}   Verb state background task
   {C992C58D-313B-469c-8202-456FF574FF4E}   CLSID_HomeGroupComponentList
   {C9A14CDA-C339-460B-9078-D4DEBCFABE91}
   {C9BC92DF-5B9A-11D1-8F00-00C04FC2C17B}   ComponentDataImpl Class
   {C9E37C15-DF92-4727-85D6-72E5EEB6995A}   SpUncompressedLexicon Class
   {c9ea5d14-cef7-4e37-851a-8043f0fb74e9}   PIN Retry UI class
   {C9F5FE02-F851-4EB5-99EE-AD602AF1E619}   StreamBufferSource
   {CA0AC604-8EF2-448A-AE97-62A2C2CC3C46}   SpDMOAudioIn Class
   {CA116708-1727-4E71-93F5-CA43081DC62A}   Device Setup Status Extension
   {ca1575f8-bf1e-4c2f-a1f9-b3aa45c92794}   Microsoft IME Software Keyboard Applet
   {CA22F5B1-E06F-4A2B-94FC-21E87FE53781}   GameUpdateTask Class
   {CA236752-2E77-4386-B63B-0E34774A413D}
   {ca24c16a-24e8-4d7c-80e8-c546d9fb2abe}
Windows.Devices.Enumeration.DeviceConnectionChangeTriggerDetails
   {CA2AF3B4-C15E-412b-B453-557746675FB7}   WmiPerf Instance Provider
   {ca34fe0a-5722-43ad-af23-05f7650257dd}   ADPCM ACM Wrapper MFT
   {CA38D8DA-C75D-11D1-8F99-00600895E7D5}   Interface Proxy Stub
   {CA38D8DB-C75D-11D1-8F99-00600895E7D5}   Interface Proxy Stub
   {CA3FDCA2-BFBE-4eed-90D7-0CAEF0A1BDA1}   PSFactoryBuffer
   {ca47b0ae-6f7b-4aeb-8d57-24b3f2aa3d44}   Remove media server command
   {ca767aa8-9157-4604-b64b-40747123d5f2}   RegistryIdleBackupHandler
   {CA80BE9F-02DB-4B14-9B52-A72D27B5FBF5}   Quiet Hours Manager Shell Service
   {ca8c87c1-929d-45ba-94db-ef8e6cb346ad}   User OOBE Create Elevated Object Server
   {CA8EB365-E97F-4cfa-965C-B3E8986ABD8F}   Media Foundation DShow Transform Wrapper
   {CAAFDD83-CEFC-4E3D-BA03-175F17A24F91}   Stream Buffer Recording Control Object
   {CAC59BFB-5547-456C-80D8-F6428C8F5456}   SpCFGEngine Class
```

Page 102

SOFTWARE OUTPUT.txt

```
{CACA7238-3C7E-4a25-AD73-DE1A4F8C7214}
{CACAF262-9370-4615-A13B-9F5539DA4C0A}
{CAE80521-F685-11d1-AF32-00C04FA31B90}    CLSID_OENote
{CB0FC8E5-686A-478B-A252-FDECF8E167B7}    scanprofilemgr class
{CB17E772-E1CC-4633-8450-5617AF577905}
{CB18B8D1-12E4-4AFD-886E-94AEFE1C70D5}    RASGCW Custom UI Class
{CB1DFE3A-EDFF-4d1f-867D-8ADB02926F4B}    OpenSearch Description Create Search
Connector Verb Handler
{cb25220c-76c7-4fee-842b-f3383cd022bc}    EnhancedStorageSilo Class
{CB39A782-E5E4-11D1-8CC0-00C04FC3261D}    RegDBCompensator Class
{CB46E850-FC2F-11D2-B126-00805FC73204}    PSFactoryBuffer
{CB6E2B90-25FA-4F08-B46C-696F5A2B6CA5}    SppWmiTokenActivationSigner
{cb82ea12-9f71-446d-89e1-8d0924e1256e}    PINLogonProvider
{CB8555CC-9128-11D1-AD9B-00C04FD8FDFF}    WbemAdministrativeLocator Class
{CB8C13E4-62B5-4C96-A48B-6BA6ACE39C76}
{cba9e78b-49a3-49ea-93d4-6bcba8c4de07}    Mpeg43 Decoder DMO
{CBC04AF1-25C7-4A4D-BB78-28284403510F}    tiledatamodelsvc
{CBD30858-AF45-11D2-B6D6-00C04FBBDE6E}    TV: Pluggable Protocol
{CBE0FED3-4B91-4E90-8354-8A8C84EC6872}    CLSID_ThumbnailStreamCache
{CBEA848D-9741-4235-BDEE-DC86C5A6FF85}    CLSID_MIMERfc2047Decoder
{CC07F1AC-9ADD-4DEF-93DF-6F755F2A88A1}    DataExchange Host
{CC1101F2-79DC-11D2-8CE6-00A0C9441E20}    MediaLocator Class
{CC19079B-8272-4D73-BB70-CDB533527B61}    HNetCfg.FwProducts
{CC23F537-18D4-4ECE-93BD-207A84726979}    MSVidCtl FilePlayback to Audio Renderer
Composition Segment
{CC3FA696-93B8-4745-B935-0599ACB97747}    Close Search Tab Command
{CC48A47F-EFD6-4925-A515-28C40C5A78B6}    MSASR Locale Handler Class (1041)
{CC55EE92-FE67-43C9-95E7-E646918A4A04}    Enhanced Storage Command Handler
{CC58E280-8AA1-11D1-B3F1-00AA003761C5}    Smart Tee Filter
{CC58E281-8AA1-11D1-B3F1-00AA003761C5}    DirectX Transform Wrapper
{CC6EEFFB-43F6-46c5-9619-51D571967F7D}    Web Publishing Wizard
{CC6F1005-CAE0-4892-B602-65A5FD7EC2D6}    CLSID_HomeGroupCollection
{CC785860-B2CA-11CE-8D2B-0000E202599C}    MPEG Audio Decoder Property Page
{CC7BFB42-F175-11d1-A392-00E0291F3959}    Video Effect (1 input) Class Manager
{CC7BFB43-F175-11d1-A392-00E0291F3959}    Video Effect (2 input) Class Manager
{CC829A2F-3365-463F-AF13-81DBB6F3A555}    BDA Tuning Model Channel ID Tuning Space
{CC89BA65-661C-494a-85C0-5D697DFEB30C}    Ribbon delete command
{CC9072AB-C000-49D8-A5AA-00266C8DBB9B}    Microsoft WBEM _IWbemEnumMarshaling
Enumerator Helper
{CCAA63AC-1057-4778-AE92-1206AB9ACEE6}    StreamBufferRecordingAttributes
{CCAE9D9B-E430-4454-8949-666D9F739994}    WindowTreeCache Class
{CCAEAA6D-3A50-488F-A664-5FACF424BC46}    State of homegroup commands
{ccb1d8cb-d39f-41c9-b793-0196214bdc4e}    IMECFM
{CCB4EC60-B9DC-11D1-AC80-00A0C9034873}    PDPO Class
{ccc63ae1-56a5-4f9c-abe8-e55674f0c0a6}    CRandomAccessStreamReferenceProxy
{CCC8D08D-DD79-4550-8F3E-C57D4F8A5F40}    PSFactoryBuffer
{CCDEDADE-AE23-47f3-A588-B09A05CA1A00}    DcpSearchTargetServices
{CCE1CB19-F9B3-4017-9541-DDA1B03F9A43}
{CCEC11F2-00C4-4266-9932-B9E49442711E}    Open Command
{CD000001-8B95-11D1-82DB-00C04FB1625D}    CDOMessage Class
{CD000002-8B95-11D1-82DB-00C04FB1625D}    CDOConfiguration Class
{CD000004-8B95-11D1-82DB-00C04FB1625D}    CDO DropDirectory class
{CD000005-8B95-11D1-82DB-00C04FB1625D}    SMTP OnArrival Script Host Sink Class
{CD000006-8B95-11D1-82DB-00C04FB1625D}    NNTP OnPost Script Host Sink Class
{CD000007-8B95-11D1-82DB-00C04FB1625D}    NNTP OnPostFinal Script Host Sink Class
{CD000008-8B95-11D1-82DB-00C04FB1625D}    SMTPConnector Class
{CD000009-8B95-11D1-82DB-00C04FB1625D}    NNTPPostConnector Class
{CD000010-8B95-11D1-82DB-00C04FB1625D}    NNTPFinalConnector Class
{CD000011-8B95-11D1-82DB-00C04FB1625D}    NNTPEarlyConnector Class
{CD000012-8B95-11D1-82DB-00C04FB1625D}    NNTP OnPostEarly Script Host Sink Class
{CD12A3CE-9C42-11D2-BEED-0060082F2054}    ClientNetManager Class
{CD184336-9128-11D1-AD9B-00C04FD8FDFF}    WbemAuthenticatedLocator Class
{CD1ABFC8-6C5E-4A8D-B90B-2A3B153B886D}    Microsoft WBEM
```

Page 103

SOFTWARE OUTPUT.txt

```
_IWbemConfigureRefreshingSvc Configure Refreshing Services Factory
 {cd3aa379-93f4-421b-9802-aeab68b06771}  RdpVideoSink Class
 {CD3AFA70-B84F-48F0-9393-7EDC34128127}  APPLICATION__X_MPLAYER2 Moniker Class
 {CD3AFA71-B84F-48F0-9393-7EDC34128127}  APPLICATION__X_MS_WMZ Moniker Class
 {CD3AFA72-B84F-48F0-9393-7EDC34128127}  AUDIO__AIFF Moniker Class
 {CD3AFA73-B84F-48F0-9393-7EDC34128127}  AUDIO__BASIC Moniker Class
 {CD3AFA74-B84F-48F0-9393-7EDC34128127}  AUDIO__MID Moniker Class
 {CD3AFA76-B84F-48F0-9393-7EDC34128127}  AUDIO__MP3 Moniker Class
 {CD3AFA77-B84F-48F0-9393-7EDC34128127}  AUDIO__MPEG Moniker Class
 {CD3AFA78-B84F-48F0-9393-7EDC34128127}  AUDIO__MPEGURL Moniker Class
 {CD3AFA7A-B84F-48F0-9393-7EDC34128127}  AUDIO__SCPLS Moniker Class
 {CD3AFA7B-B84F-48F0-9393-7EDC34128127}  AUDIO__WAV Moniker Class
 {CD3AFA7C-B84F-48F0-9393-7EDC34128127}  AUDIO__MP4 Moniker Class
 {CD3AFA7D-B84F-48F0-9393-7EDC34128127}  AUDIO__VND_DLNA_ADTS Moniker Class
 {CD3AFA7E-B84F-48F0-9393-7EDC34128127}  AUDIO__MKA Moniker Class
 {CD3AFA7F-B84F-48F0-9393-7EDC34128127}  AUDIO__FLAC Moniker Class
 {CD3AFA83-B84F-48F0-9393-7EDC34128127}  AUDIO__X_MS_WAX Moniker Class
 {CD3AFA84-B84F-48F0-9393-7EDC34128127}  AUDIO__X_MS_WMA Moniker Class
 {CD3AFA88-B84F-48F0-9393-7EDC34128127}  VIDEO__AVI Moniker Class
 {CD3AFA89-B84F-48F0-9393-7EDC34128127}  VIDEO__MPEG Moniker Class
 {CD3AFA8F-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_ASF Moniker Class
 {CD3AFA90-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_ASF_PLUGIN Moniker Class
 {CD3AFA92-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_WM Moniker Class
 {CD3AFA93-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_WMX Moniker Class
 {CD3AFA94-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_WMV Moniker Class
 {CD3AFA95-B84F-48F0-9393-7EDC34128127}  VIDEO__X_MS_WVX Moniker Class
 {CD3AFA96-B84F-48F0-9393-7EDC34128127}  APPLICATION__X_WMPLAYER Moniker Class
 {CD3AFA97-B84F-48F0-9393-7EDC34128127}  AUDIO__3GPP Moniker Class
 {CD3AFA98-B84F-48F0-9393-7EDC34128127}  AUDIO__3GPP2 Moniker Class
 {CD3AFA99-B84F-48F0-9393-7EDC34128127}  VIDEO__MP4 Moniker Class
 {CD3AFA9A-B84F-48F0-9393-7EDC34128127}  VIDEO__QUICKTIME Moniker Class
 {CD3AFA9B-B84F-48F0-9393-7EDC34128127}  AUDIO__VND_MPEG_TTS Moniker Class
 {CD3AFA9C-B84F-48F0-9393-7EDC34128127}  VIDEO__MKV Moniker Class
 {CD3AFA9D-B84F-48F0-9393-7EDC34128127}  VIDEO__MK3D Moniker Class
 {cd4b7782-eb37-4bfe-b9ce-685f634a08dc}  CSdWhcNotifier Class
 {CD5096A1-E7E7-4E09-8B12-CBF2790A87CF}  Bluetooth Personal Area Connection
Enumerator
 {CD6C7868-5864-11D0-ABF0-0020AF6B0B7A}  CTreeView Control
 {CD70A734-B6DB-4588-9813-FF2E37A4661F}  WorkspaceBrokerAx Class
 {CDA42200-BD88-11D0-BD4E-00A0C911CE86}  Filter Mapper2
 {CDA8ACB0-8CF5-4F6C-9BA2-5931D40C8CAE}  FaxServer Class
 {CDBD8D00-C193-11D0-BD4E-00A0C911CE86}  CMediaPropertyBag
 {CDBEC9C0-7A68-11D1-88F9-0080C7D771BF}  Event Class
 {cdc32574-7521-4124-90c3-8d5605a34933}  Windows Media Player Burn Audio CD Handler
 {CDC7B0EB-EE28-4914-9128-64689D3F34F0}  Connected Account Services Factory
 {CDC82860-468D-4d4e-B7E7-C298FF23AB2C}  ShellItemArray Shell Namespace helper
 {cde7427e-9d90-4788-8415-765c156c9bc2}  PSFactoryBuffer
 {CE264EED-3CD3-4BC5-9774-D3A18BE9B0F2}  ResourceValidator Class
 {CE2BB7DC-73F3-482F-90B6-5BFAA04D0157}  SpRecoMaster Class
 {ce2f5d02-a575-4f4c-ad73-34baf96f8512}  PSFactoryBuffer
 {CE47E952-2ADE-45b9-8F64-F829BB4BAA34}  NarratorDataItem Class
 {CE510457-55EC-4f86-91BE-323BC91AC34F}  Shell User Domain Enumeration Object
 {ce8dbe60-d37a-4bdd-ab3a-399e69489182}
 {CECAD1B6-9620-4295-93C6-85B305D82AE4}  Optional Features Admin Helper
 {CED43EC3-71D3-4534-826E-D499608BA83F}  User Session Toast Manager
 {CEEE3B62-8F56-4056-869B-EF16917E3EFC}  Microsoft IMAPI v2, .ISO Image Manager
utility
 {ceefea1b-3e29-4ef1-b34c-fec79c4f70af}  New Shortcut Wizard
 {ceff45ee-c862-41de-aee2-a022c81eda92}  CLSID_SeparateSingleProcessExplorerHost
 {CF0E916A-DA25-49CA-A264-1D41C009EED0}  ProtocolWithResultsActivatedEventArgs
 {CF0F2F7C-F7BF-11d0-900D-00C04FD9189D}  MtStream Class
 {CF1BF3B6-7AD0-4410-996B-C78EAFCD3269}  Windows Markup File
 {CF2CF428-325B-48d3-8CA8-7633E36E5A32}  AD RMS Rights Policy Template Management
```

Page 104

SOFTWARE OUTPUT.txt

```
(Automated) Task Handler
    {CF3D2E50-53F2-11D2-960C-00C04F8EE628}    SpMMAudioIn Class
    {cf4270f5-2e43-4468-83b3-a8c45bb33ea1}    Proactive Scan
    {CF49D4E0-1115-11CE-B03A-0020AF0BA770}    AVI Decompressor
    {CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}    WbemDefaultPathParser
    {cf572d73-d6e5-4d45-acad-f18f4f76656f}    CLSID_AppsFolderThumbnailProvider
    {CF67796C-F57F-45f8-92FB-AD698826C602}    .contact shell context menu
    {CF948561-EDE8-11CE-941E-008029004347}    System Monitor Data Properties
    {CFA8E0EF-DFC7-49EA-9C1C-827FF9B1168F}    lockframework
    {cfb16474-0a2e-48dc-88ce-8c0adb7e5e46}    Windows Media Player Device Options
Property Page
    {CFBFAE00-17A6-11D0-99CB-00C04FD64497}    Microsoft Url Search Hook
    {CFC399AF-D876-11D0-9C10-00C04FC99C8E}    Msxml
    {CFC44584-E947-47fe-B9C4-99168114C866}    CParmNode
    {CFC81939-3886-4ACF-9692-DA58037AE716}    MSAppData Scheme Handler
    {CFCCC7A0-A282-11D1-9082-006008059382}    Darwin App Publisher
    {cfd82661-9b9e-4c87-9dcb-e0fd11681b44}    CLSID_AppContentXmlPropertyStore
    {CFF49D53-EE51-49F2-A807-7E3DF4EA36E3}    WSecEdit Local Security Settings Class
    {CFF9990B-6414-43F1-A526-14EA5EEAFBDA}    Library Share Engine
    {D01B8F28-0BD1-4652-A415-8229F5EE506C}    PSFactoryBuffer
    {D02AAC50-027E-11D3-9D8E-00C04F72D980}    Collection of all the available BDA Tuning
Model Tuning Space objects on this system
    {D034B02A-093B-46B7-8C75-61B9104C71E9}    Lock Screen Slideshow Host
    {d044309b-5da6-4633-b085-4ed02522e5a5}    App Content File Persistent Handler
    {D049B20C-5DD0-44FE-B0B3-8F92C8E6D080}
    {D0520B5D-1B5F-4ECF-A940-6E57476AE4B0}
    {D0565000-9DF4-11D1-A281-00C04FCA0AA7}    EventSystem.EventObjectChange
    {d064d602-c470-4162-8ae6-880edc553b89}    DeviceInformationUpdateServer
    {d0b7e02c-e1a3-11dc-81ff-001185ae5e76}    DiagnosticProfile
    {d0da2915-3f89-4519-a4ca-5e02528c8ec4}    PlaylistDocument
    {D0E55F9F-0021-42fe-A1DB-C41F5B564EFE}    RASMapi Class
    {D105A4D4-344C-48EB-9866-EE378D90658B}    CLSID_HomeOperationSink
    {D1202225-F099-47FE-A965-8A78ABD6DE7D}
    {D13E3F25-1688-45A0-9743-759EB35CDF9A}    AcquisitionManager Class
    {D1456EF1-172B-49C0-8CB7-FAC3C01AB446}    PSFactoryBuffer
    {D1621129-45C4-41AD-A1D1-AF7EAFABEEDC}    WIA Default UI
    {D1681A3F-DA52-4B58-901A-407C3158B1E2}    Usb_Capability_Handler_Class
    {D169C14A-5148-4322-92C8-754FC9D018D8}    rtf persistent handler for mapi email
    {D16B87DE-029E-4C85-92C8-ED8BBC5E882C}    Microsoft Embedded Search Gatherer Inline
Notification
    {D17D1D6D-CC3F-4815-8FE3-607E7D5D10B3}    Text to Speech Control Panel
    {D183B45C-8099-4cd3-BE91-2441E5906738}    NarratorTreeViewItem Class
    {D18705BE-FC2F-44C8-AEFF-1CD49AEA8FC1}    CLSID_NotificationSettings
    {D1915118-9D27-4C69-B82E-7955DAF57201}    SpUncompressedLexicon Class
    {d1934e71-740b-47cf-b051-6551e5b80fd5}    Drive Backup Command
    {D194386A-04E3-4814-8100-B2B0AE6D78C7}    VideoFrameNativeFactory
    {d1a42999-0adf-11da-b070-0011856571de}
    {D1C5A1E7-CC47-4E32-BDD2-4B3C5FC50AF5}    Slide
    {D1E460DC-A564-4B5F-8B7D-CA3C1AC0C27C}    PhoneShareHost
    {D1E7EE36-6AA6-4dc2-90BB-16A722623B7D}    OOBE PID Plugin
    {D1F447C5-D55A-4149-A364-52EB93D7B2F9}    PSFactoryBuffer
    {D1FE6762-FC48-11D0-883A-3C8B00C10000}    DXTransformFactory Class
    {D2035EDF-75CB-4EF1-95A7-410D9EE17170}    DLNA Content Directory Data Source
    {d20a3293-3341-4ae8-9aaf-8e397cb63c34}    DefragEngine Class
    {D20EA4E1-3957-11d2-A40B-0C5020524153}    Administrative Tools
    {D215781D-019E-4FA0-903D-0CDCDE13A4F5}    Winmgmt MOF Compiler OOP
    {D23B1E3C-A750-422C-8314-2333F8936EBE}    HighlightCursor Class
    {d23b90d0-144f-46bd-841d-59e4eb19dc59}    WMVideo9 Encoder DMO
    {d23e6477-b104-4707-81cb-e1ca19a07016}    Video Renderer Activate
    {D2423620-51A0-11D2-9CAF-0060B0EC3D39}    XML Parser
    {D245983C-67FC-4923-AA19-3F048C495E8B}    MbaeManagerInternal Class
    {D2517915-48CE-4286-970F-921E881B8C5C}    Windows Live Sign-in Control
    {D25D8842-8884-4A4A-B321-091314379BDD}    UIAnimationManager2
```

Page 105

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {D269BF5C-D9C1-11D3-B38F-00105A1F473A} | WBEM Scripting Refresher |
| {D26AA4A5-92AD-48DB-8D59-95EF0DCE6939} | CMigrationPlugin Object |
| {d26c7a0a-83a0-48d3-9174-529db999b4a4} | PSFactoryBuffer |
| {D26DE5C1-C061-43F7-9C40-7517526CF1C1} | Startup App Check Provider |
| {D277DF13-EB33-47e1-A3B9-0AC04B1F24F4} | MCCSPopSyncEngine |
| {D27CDB6E-AE6D-11cf-96B8-444553540000} | Shockwave Flash Object |
| {D27CDB70-AE6D-11cf-96B8-444553540000} | Macromedia Flash Factory Object |
| {d284acc0-ceed-46cc-9484-38709e695510} | JpnRankerDS Class |
| {D2942F8E-478E-41D3-870A-35A16238F4EE} | Console Shortcut Property Sheet Handler |
| {D2AC2892-B39B-11D1-8704-00600893B1BD} | DirectMusicLoader |
| {D2C13906-51EF-454e-BC67-A52475FF074C} | SpW3CGrammarCompiler Class |
| {d2cdd0e2-bf87-41b1-a9ee-ab94c072ddf7} | CUICCHandler |
| {D2D588B5-D081-11D0-99E0-00C04FC2F8EC} | WDM Instance Provider |
| {D2D79DF5-3400-11d0-B40B-00AA005FF586} | IVolumeClient_PSFactory |
| {D2D79DF7-3400-11d0-B40B-00AA005FF586} | IDMNotify_PSFactory |
| {d2e86c4f-ea06-4a89-bf00-b49706db46e6} | DDO Resource Info |
| {d2ea46a7-c2bf-426b-af24-e19c44456399} | Microsoft RDP Client Control - version 7 |
| {D2EC4F1C-F91E-4F58-9329-016E444FD199} | InkRecognizers Class |
| {D2ED260C-38F1-4ABE-8B2B-D4A088C54416} | PSFactoryBuffer |
| {D3075F87-A7BD-4231-9F6A-60C5E07374A7} | |
| {D313A859-B510-461A-B4A7-70FF73AEF1F1} | DeviceAccessPolicyCheck |
| {d3162b92-9365-467a-956b-92703aca08af} | |
| {D31B6A3F-9350-40DE-A3FC-A7EDEB9B7C63} | WMI instrumentation: |
| Win32_SystemConfigurationChangeEvent | |
| {D32CD718-970D-4496-B7A7-337BE8890145} | Taskbar Setting Handler |
| {d34a6ca6-62c2-4c34-8a7c-14709c1ad938} | Common Places FS Folder |
| {D34BD150-6D84-443E-83EE-04C7682377E4} | Unsecured Net Connect Control Class |
| {D34BD155-6D84-443E-83EE-04C7682377E4} | Pre-CFE Page Class |
| {D3588AB0-0781-11CE-B03A-0020AF0BA770} | AVI/WAV File Source |
| {D36D2090-4DF3-4bd4-A22F-0D91975F7964} | SpMSSemanticInterpretation Class |
| {D385FDAD-D394-4812-9CEC-C6575C0B2B38} | |
| {d3c0b79d-0fd2-4b5d-9bf6-5e41d6f15c08} | App Content Filter |
| {D3C4B7DB-E7BB-4778-89A2-E4B0EE41C29F} | SpMemoryStream Class |
| {d3ca534d-3342-42b2-900b-1aceaff85e8a} | CLSID_SearchServices |
| {D3D742AB-0446-43C0-9899-1084DA4406FF} | NarratorCommandEventInproc Class |
| {D3DCB472-7261-43ce-924B-0704BD730D5F} | WS Discovery Provider Class |
| {D3E34B21-9D75-101A-8C3D-00AA001A1652} | Paintbrush Picture |
| {D406E841-B82A-4790-99A8-975768E37157} | PSFactoryBuffer |
| {d41748f8-737c-4edb-bb21-18d8b37c511e} | CLSID_PickerControllerInProcServer |
| {d43f6fd5-904a-407f-97bc-5f8be75f532d} | Play To Menu Command |
| {D44377B8-1F2F-4FAA-9C8E-6C4AD2928E47} | Hybrid Drive Cache Rebalance Task |
| {D4480A50-BA28-11d1-8E75-00C04FA31A86} | Add Network Place |
| {d450a8a1-9568-45c7-9c0e-b4f9fb4537bd} | Installed Updates |
| {D451359E-D6F4-45BB-8A05-271E8A98C740} | Sync Mappings Command State Handler |
| {D46443F6-133B-4938-9C52-23B9EDD62CC3} | FullScreen Positioner |
| {D4692569-5A04-351D-8BA7-5F43AB458DF6} | |
| {D46A0B4F-4EEC-4A83-8DE5-9C86F0DFA34D} | Setting Sync WLS Notifier Shell Service Object |
| {D4B30741-9639-456D-99C5-6F223AE5EB20} | CLSID_MIMEMailbox |
| {D4C4F382-D9B2-41C9-8817-0DA701BB213B} | DsmDevice Class |
| {D4CA0E2D-6DA7-4b75-A97C-5F306F0EAEDC} | Packed Property Storage Object (marshal by value) |
| {D4DCD3D7-B4C2-47D9-A6BF-B89BA396A4A3} | |
| {D4EFF9CD-16DE-446e-83C5-9537543CF4A1} | Set User Defaults Control Panel |
| {d4f01ada-979c-491e-bac3-cd3c0e7bcf82} | Online Id Filter |
| {D4F4D30B-0B29-4508-8922-0C5797D42765} | WIA Default Segmentation Filter |
| {D4FA3D55-FAE9-4F35-A3B5-0E26D98933AC} | NotificationObjFactory |
| {D5029E5D-F109-4BC0-B6DB-07F92D6ABAE7} | SpPLSLexcicon Class |
| {d509c21a-b88c-4ad1-8fad-d6a7572728e5} | Search Clear MRU Command |
| {D5120AA3-46BA-44C5-822D-CA8092C1FC72} | |
| {D51BD5A1-7548-11CF-A520-0080C77EF58A} | Wave Parser |
| {D51BD5A2-7548-11CF-A520-0080C77EF58A} | MIDI Parser |
| {D51BD5A3-7548-11CF-A520-0080C77EF58A} | Multi-file Parser |

Page 106

SOFTWARE OUTPUT.txt

```
{D51BD5A5-7548-11CF-A520-0080C77EF58A}  File stream renderer
{D5307D61-F9BC-4de1-94EA-1DEF24DF4BB2}
{d53cd902-7edc-430f-a1e0-c38c01b6fe8b}  Microsoft IME Japan IH Suggestion Data
Source
{d54378cd-91d8-4e10-a00b-819f9a9efcb1}  CoFilterPipeline Class
{D54EEE56-AAAB-11D0-9E1D-00A0C922E6EC}  Microsoft InfoTech IStorage for Win32
Files
{D555645E-D4F8-4c29-A827-D93C859C4F2A}  Ease of Access
{D5753BBB-C5A8-4F50-9D81-210BAB0C5FB6}  Mpeg-2 Stats
{d58960ba-2ef3-4910-9e34-c911b1710180}  ShellTravelLog
{D593A7D5-658F-4FE1-9D05-0B13E10D1A12}  WebProviderError Object
{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}  SENS Network Events
{D5978630-5B9F-11D1-8DD2-00AA004ABD5E}  SENS Logon Events
{D5978640-5B9F-11D1-8DD2-00AA004ABD5E}  SENS OnNow Events
{D5978650-5B9F-11D1-8DD2-00AA004ABD5E}  SENS Logon2 Events
{D5AB5662-131D-453D-88C8-9BBA87502ADE}
Microsoft.ManagementConsole.Advanced.FrameworkSnapInFactory
{D5B0F757-A97F-4311-B864-78D6094217C6}  Setting Sync Provider Services
{D5B97D79-6DC3-403d-B178-59C0930C5DAC}  DeviceConsentProvider
{D5BD69C0-5126-4721-8668-F0783F3640FB}  NarratorTableItemPattern Class
{D5C66BE1-C209-11d1-8DEC-00C04FC2E0C7}
{D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}
{D5ED6B03-EDA3-4cbc-9FF1-60182438C8F6}  WSD Print Proxy Class
{D5F7E36B-5B38-445D-A50F-439B8FCBB87A}  CLSID_WscToastActivationHandler
{D6015EC3-FA16-4813-9CA1-DA204574F5DA}  AlgController Class
{D63A1416-FCEC-4431-862F-E8056223DD03}  Windows Photo Viewer DropTarget
{D63A5850-8F16-11CF-9F47-00AA00BF345C}  WBEM Framework Instance Provider
{D63AA156-D534-4BAC-9BF1-55359CF5EC30}  Sync Center User Profile Notification
Handler
{D63B10C5-BB46-4990-A94F-E40B9D520160}  RuntimeBroker
{D63D5073-E487-4412-A003-4B3E82514E3D}
{D644A6D2-8E5E-4405-AA66-1554E9A8ED10}  RDSProfileHandler Class
{D648FEA1-EA00-4FF4-B8BD-034BD2B25A23}
{D65B9994-6416-41ED-84EE-08733558C381}  SpCompressedLexicon Class
{D66949A0-C766-48D7-B2C6-4A85382BE9C1}  MSASR Locale Handler Class (3082)
{d66c2605-9d5d-475e-a5b8-3790743ee2ff}  CDocumentPropertiesProxy
{D66D6F99-CDAA-11D0-B822-00C04FC9B31F}  Multi Language ConvertCharset
{D6707039-94AB-490A-95D6-C268524D8B8F}  SpDataKey Class
{D6791A63-E7E2-4fee-BF52-5DED8E86E9B8}  Portable Devices Menu
{D682C4BA-A90A-42FE-B9E1-03109849C423}  StreamBufferComposeRecordingObj
{D68AF00A-29CB-43FA-8504-CE99A996D9EA}  Microsoft WBEM (non)Standard Marshaling
for IWbemServices
{d69e0717-dd4b-4b25-997a-da813833b8ac}  AudioLimiter Class
{D6AC71F0-D4A7-41DD-88C4-B9985855D546}
CAppointmentsProviderInternalShowTimeFrameActivationPlugin
{D6AD10F3-70AB-41E1-96B3-4C36E35D333C}  SpRecoMaster Class
{D6EBC66B-8921-4193-AFDD-A1789FB7FF57}  PSFactoryBuffer
{D6F8EC75-A388-47de-BA3A-903B12A38E86}  PSFactoryBuffer
{D6FEDB1D-CF21-4BD9-AF3B-C5468E9C6684}  MMCVersionInfo 1.0 Object
{D707877E-4D9C-11d2-8784-F6E920524153}  User Property Pages
{D73733C8-CC80-11D0-B225-00C04FB6C2F5}  FaxServer Class
{d74a07b1-ea36-4f32-a85a-9777a4ae12aa}  PSFactoryBuffer
{D74DFA88-D5E3-41F6-B677-66FFB6591B00}  ModernShareAccount
{D751DCF1-EEAC-42b1-9593-E4B77CCB42ED}  NarratorValuePattern Class
{D753D854-4427-4F8B-AB9A-CC13167C4BC0}  Windows Connected Search Contacts Provider
{D76334CA-D89E-4BAF-86AB-DDB59372AFC2}  MSVidCtl CC to Audio Renderer Composition
Segment
{D76E9DED-E5D8-4802-8B28-4A09BDB90C3F}  Drawing
{D772327B-027D-48BE-AD01-9FD96388255F}  OOBE ComputerName Plugin
{D78C3A7D-9018-41b6-9CE3-2BFDD45D45A1}  CCharacteristicNode
{D7B70EE0-4340-11CF-B063-0020AFC2CD35}  DirectDraw Object
{d7bfd8f3-678c-4827-b84b-0e5fc6d15be3}  Add media server command
{D7C1AEB5-10F2-48cb-A182-F7EF79C51B19}  WSD Publisher
```

Page 107

SOFTWARE OUTPUT.txt

```
{D7C3453E-1F1C-48CD-AFE6-CFF2A937D337}
{d7ca55ab-5022-4db3-a599-abafa358e6f3}   MF ADTS Sink Class Factory
{D7E10D43-6CB9-4a61-91F4-9C722C265CB3}   NarratorTaskSwitchWindow Class
{D7F1C02D-48AC-40ED-8996-AF704232C9F6}   MTF Contact Harvester
{D7F9888F-E3FC-49b0-9EA6-A85B5F392A4F}   Windows Live ID Provider
{D7FCB63B-5C55-11D1-8F00-00C04FC2C17B}   SnapinAboutImpl Class
{D805F2C8-ABA9-41E8-AA22-9F7392A27E72}   NarratorTIE Class
{D82BE2B0-5764-11D0-A96E-00C04FD705A2}   IShellFolderBand
{d83e8cbe-841d-4397-b6e4-f64f2e3ab469}   CMVUIFallbackKey
{d84fa0c2-b0b3-4470-9345-75db0ec5a83a}   Universal Delegate Folder
{D8559EB9-20C0-410E-BEDA-7ED416AECC2A}   Windows Defender
{D85A2008-32B3-4747-8189-7FB809F3CFF1}   PrintDialog3D.ProxyStubFactory
{D8636558-AAF6-49c1-8171-FFA6668B65A7}   Peer Info XML
{D8775A07-C529-4EA7-B307-BA7C8CBBDA03}   CloudStorageWizard
{D8872739-DF50-4ED5-B8A7-F03DCD0DCD5A}   PSFactoryBuffer
{d88dc591-4172-4a00-a6b1-7b657d2a6643}   Home Folder Categorizer
{D899A5B9-C518-42E9-B9BD-E08BEE91A92E}   CLSID_MIMEQuotedPrintableDecoder
{d8a04f01-4570-45cc-bffa-37c79cf7208c}   Chrome Controls
{D8AC8159-ABAA-4016-BF74-DE98C5917269}   MtfIHDSConflictResolver
{D8BF32A2-05A5-44c3-B3AA-5E80AC7D2576}   DrawingAttributes Class
{D8D7A7BC-0A44-45A1-941A-C938CE6CFF05}
{D8F0F5E7-11C5-4E95-BBFF-0F110C0221C4}
{d912f8cf-0396-4915-884e-fb425d32943b}   Property Helper Object
{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}   Enhanced Storage Icon Overlay Handler
Class
{d9162b5b-ca81-476e-a310-cb32d932733c}   Password Expired UI class
{d92bd3b9-99a0-4334-a497-11bcb093e9d2}   ShellWindows Class Factory
{D93CE8B5-3BF8-462C-A03F-DED2730078BA}   Slide To Shut Down Screen
{D9403860-297F-4A49-BF9B-77898150A442}
{D94EDF02-EFE5-4F0D-85C8-F5A68B3000B1}
{D957171F-4BF9-4de2-BCD5-C70A7CA55836}   Interval Class
{D969A300-E7FF-11d0-A93B-00A0C90F2719}   New Menu Handler
{D9AAAF82-03B1-4F9F-9FD5-07D2A42C8531}   VpoContext Class
{d9b3211d-e57f-4426-aaef-30a806add397}   Shell Library API
{D9BB4CEE-B87A-47F1-AC92-B08D9C7813FC}   BDA Tuning Model Digital Cable Tuning
Space
{D9EF8727-CAC2-4e60-809E-86F80A666C91}   Secure Startup
{d9efb25b-80e9-4832-bad8-ab2186bc95b0}   IMELM
{D9F6EE60-58C9-458B-88E1-2F908FD7F87C}   SpDataKey Class
{D9F9C262-6231-11D3-8B1D-00C04FB6BD3D}   WM ASF Writer Properties
{DA13DC3D-3F88-4A85-A89E-5735588A65E5}   WsmAgent
{DA1413F9-03DB-4FBD-A49F-EF0B46E46118}   MCCSImapIdleExecutor
{da158800-7434-4410-a0cd-e497c3b4a9da}   Storage Item Thumbnail Proxy
{DA17539A-3DC3-42C1-A749-A183B51F085E}   PlayTo Source Class Factory
{da1c0281-456b-4f14-a46d-8ed2e21a866f}   Microsoft.SyncShare.SyncShareFactory Class
{DA1C5437-37A2-4A68-B6AA-8D0F8F11AD40}   MCSF
{da5a95c1-cb6b-4798-88a9-473c087d9464}   CMVMasterDatastore
{da620430-5f6c-447d-8091-c5757e275b37}   RandomAccessStream Wrapper Marshaller
{DA67B8AD-E81B-4c70-9B91-B417B5E33527}   Windows Search Shell Service Object
{da7e4657-8fa8-4b76-9a14-9bf380fa3738}   CImeSearchProvidersInfo Class
{DA825E1B-6830-43D7-835D-0B5AD82956A2}   DirectPlay8Server Object
{DA93E903-C843-11D2-A084-00C04F8EF9B5}   SpGramCompBackEnd Class
{DAB7CCB2-EC94-4c7e-AB52-826D6ACD5249}   CResultTracker
{DAC9F469-0C67-4643-9258-87EC128C5941}   SREngine Class
{DACA056E-216A-4FD1-84A6-C306A017ECEC}   AMMonitoring WMI Provider
{dacfcde5-4790-45ea-a357-a8388c6a587b}
Windows.Media.Devices.Internal.CallControlBroker
{daf95313-e44d-46af-be1b-cbacea2c3065}   CLSID_StartMenuProviderFolder
{DAFD8210-5711-4B91-9FE3-F75B7AE279BF}   DirectSoundGargleDMO
{DB082FF5-F7BA-4C88-8589-3760FCB59248}   CLSID_AboveLockActivationManager
{DB263a60-8EA8-454A-B63F-82106F6993D0}   CLSID_MIMEBase64Encoder
{DB49BBEB-C744-49F8-81AC-AF97669D4CB0}   PrinterStatusHTMLViewExtension Class
{DB5286F5-C166-4032-95E2-70D62C8D26DA}   WebAccountProvider Object
```

Page 108

SOFTWARE OUTPUT.txt

```
{DB5D1FF4-09D7-11D1-BB10-00C04FC9A3A3}   FILEMGMT 1.0 Object
{DB5D1FF5-09D7-11D1-BB10-00C04FC9A3A3}   SvcVwr 1.0 Object
{db6efb73-5153-43b7-8078-c6ffc4c0238c}   CLSID_CheckCompositionCycles
{DBC85A2C-C0DC-4961-B6E2-D28B62C11AD4}   GameStatistics Class
{DBCE7E40-7345-439D-B12C-114A11819A09}   MrtResourceManager Class
{DBFCA500-8C31-11D0-AA2C-00A0C92749A3}   DiskManagement.SnapInComponent
{DC0C0FE7-0485-4266-B93F-68FBF80ED834}   Microsoft DVBC Network Provider
{DC1C5A9C-E88A-4dde-A5A1-60F82A20AEF7}   File Open Dialog
{dc28a608-b55f-46ff-b0db-e2c85b332463}   ApplicationActivationImpl
{DC357AD1-94F3-4932-80D4-306B69004B46}   Extrinsic Property Store Handler
{DC626A64-D684-4627-83CB-44420ABDBD1A}   SpSharedRecoInst Class
{DC651A43-0720-4a2b-9971-BD2EF1329A3D}   IE Component Categories conditional cache
daemon
{DC664FDD-D868-46EE-8780-8D196CB739F7}
{DC714A79-D4B7-472C-A390-3FCC6D9E9FB7}   CLSID_BackgroundAccessApplications
{DC79858F-F8D2-47F7-9A1E-C879CB59A4F9}   Digital Keystone BDA Proxy Persistence
Manager
{DC79A5C8-CCAD-4698-9034-C4C8068011C5}   PSFactoryBuffer
{DC7A02CD-2E47-406C-BA5A-B08EC00C4238}   MAPISendMailServer
{DC923725-0FDD-45E1-AE74-EA09182E739B}   Microsoft WBEM Wbem Token Cache
{DCA55752-E6D5-4080-8E35-A21546DA8295}   iotassignedaccesslockframework
{DCB00009-570F-4A9B-8D69-199FDBA5723B}   Network List Manager Public Proxy
{DCB00C01-570F-4A9B-8D69-199FDBA5723B}   NetworkListManager
{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1}   speechtextservice class
{DCBFB8FA-CD19-4F1C-A27D-23AC706DED72}   Microsoft LLDP Notify Object
{DCC42FB9-F88D-43C2-B874-727DF0F75586}   OOBE DUI Wizard
{dccc0bed-6066-11d1-8c13-00c04fd8d503}   Microsoft Organization Extension
{DCED8DB0-11A5-4b16-AB9D-4E28CA38C99F}   Advanced Configuration Dialog
{DCF33DF4-B510-439F-832A-16B6B514F2A7}   Microsoft WBEM _IWbemRefresherMgr
Refresher Cache Factory
{DCFD3EA8-D960-4719-8206-490AE315F94F}   Data Integrity Scan
{DD06A84F-83BD-4d01-8AB9-2389FEA0869E}   Dot11 AdHoc Manager
{DD13DE77-D3BA-42D4-B5C6-7745FA4E2D4B}   MotionBlur
{DD1432D7-B76B-4227-9C57-D82E9D844441}   CRootWAPNodeProcessor
{DD313E04-FEFF-11d1-8ECD-0000F87A470C}   User Assist
{DD468E14-AF42-4D63-8908-EDAC4A9E67AE}   Create and edit Wireless policies
{DD522ACC-F821-461A-A407-50B198B896DC}   HardwareDeviceNotif
{dd5cf606-9ea7-49e1-8e82-b789e4443b4f}   MS-IME Handwriting Applet
{DD75716E-B42E-4978-BB60-1497B92E30C4}   text persistent handler for mapi email
{dd767e9d-cc0f-47b1-8f27-bb890491339d}   PlayToReceiver Launcher class
{DD7CE375-32BC-47a6-B816-AB70DF782969}   NarratorRadioButton Class
{DDACC952-01A7-4D00-8809-EEEE479779BC}   DeviceStatus
{DDC05A5A-351A-4E06-8EAF-54EC1BC2DCEA}   Application Frame
{DDC0EED2-ADBE-40b6-A217-EDE16A79A0DE}   GenericFilter
{ddcc6bb8-4cd6-462a-9289-d82d2bee1ffd}   Navigation Pane Show All Folders Explorer
Command
{ddcd33d7-f53c-4554-a71f-f86f49079827}   Windows.Media.Devices
{ddcfd26b-feed-44cd-b71d-79487d2e5e5a}   SRUM COM Server
{DDD6F54C-326E-44c1-9CFC-C89D997FFCCD}   NarratorTablePattern Class
{DDE33513-774E-4BCD-AE79-02F4ADFE62FC}
{DDE5783A-88B9-11d2-84AD-00C04FA31A86}
{DDECE4B2-979F-4CDB-9F58-B036FE5A510C}   Firewall Control Panel
{DE010DA1-289B-4232-8CD0-5112DCA6A7B3}   Microsoft Virtual Disk Service Basic
Provider
{de2d022d-2480-43be-97f0-d1fa2cf98f4f}   Provides IPortableDeviceKeyCollection
helper methods for portable devices applications and drivers
{DE3F3560-3032-41B4-B6CF-F703B1B95640}   Windows Search Service Profile Notify
Handler
{de434264-8fe9-4c0b-a83b-89ebeebff78e}
{DE4874D1-FEEE-11d1-A0B0-00C04FA31A86}
{DE4874D2-FEEE-11d1-A0B0-00C04FA31A86}
{de50c7bb-faa7-4a7f-ba47-bf0efcfe433d}
{de54af92-ead8-4a7e-88ab-135b6e1a3a23}   Windows.System.Profile.HardwareId
```

Page 109

SOFTWARE OUTPUT.txt

```
{DE75D012-7A65-11D2-8CEA-00A0C9441E20}   DxtJpeg Class
{DE77BA04-3C92-4d11-A1A5-42352A53E0E3}   Home Group Member Status
{DE7D3D65-5454-4EF5-9518-776739DAB39F}   LockScreen Call Broker
{DE815B00-9460-4F6E-9471-892ED2275EA5}   RecoManager Class
{DE83650F-8CE4-40EA-A08E-6F0E5CD46F6B}   Device Graph Object Cache Manager Class
{DE9C1288-0F09-40ff-BA84-7F19279FA74B}   Idenity Listener CLSID
{DEA8AFA0-CC85-11D0-9CE2-0080C7221EBD}   Create and edit Internet Protocol Security
policies
{DEA8AFA1-CC85-11D0-9CE2-0080C7221EBD}   Create and edit Internet Protocol Security
policies
{DEA8AFA2-CC85-11D0-9CE2-0080C7221EBD}   Create and edit Internet Protocol Security
policies
{DEB01010-3A37-4d26-99DF-E2BB6AE3AC61}   IVolumeClient4_PSFactory
{deca92e0-af85-439e-9204-86679978da08}   EDP Policy Manager Task Handler
{DECBDC16-E824-436e-872D-14E8C7BF7D8B}   RtpObject Class
{dedf110a-8df2-4a67-b18d-b3b3dda7474f}   ExternalAccountAccessor
{DEEF2A9B-B3B7-46F2-A07F-D53340BF9E0F}   CLSID_SettingSyncDiagnostics
{DEF03231-9688-11E2-BE7F-B4B52FD966FF}   Device Driver Disk Cleanup Handler
{DEF03232-9688-11E2-BE7F-B4B52FD966FF}   Plug and Play Maintenance Task
{def065bd-a9fa-402b-8775-ab48d88775db}   Compatibility Policy Manager
{DF0B3D60-548F-101B-8E65-08002B2BD119}   PSSupportErrorInfo
{DF1E92F3-F333-4EF5-9C38-B75CB65FFC39}   Windows.Globalization
{DF24A1AC-F041-4E59-B7DA-EB2634A93CFE}   F12AppFrameClient
{DF2FCE13-25EC-45bb-9D4C-CECD47C2430C}   CUri
{DF46C02A-3568-4765-AAD3-88F5E1D42F92}   Search Filter Kind Command
{df46cd07-4f86-42f0-8fa9-35c3ce55d77b}
{DF5196F5-203A-4EDF-BE7E-D08E5906B1CF}   File Change Tracker Registrar
{DF5440C1-FFB1-4F14-99A9-D692CC978E07}   SceneAnalysisMFT
{DF5C33B8-3120-4cd4-991F-300385B66FDE}   NarratorImage Class
{DF60686C-2941-4893-80C0-F13173B719D3}   HomeGroup State
{df6775de-380d-4c14-8b62-fb69912e6d30}   Function Discovery USB Provider
{df6b5e0d-ff61-4cdd-b181-1c6f88315f87}   ImeLmJpn
{DF9144AE-8785-4B2B-93AD-A775CE6B6C42}   SpGrammarCompiler Class
{DFA22B8E-E68D-11d0-97E4-00C04FC2AD98}   SQLOLEDB Enumerator
{DFD74844-990B-4410-9DA0-2848EFA85D14}   WMPlayer ClipPropPage Class
{DFE49CFE-CD09-11D2-9643-00C04f79ADF0}   Cabview Data Object
{DFFACDC5-679F-4156-8947-C5C76BC0B67F}   delegate folder that appears in Users
Files Folder
{DFFFAE4D-F0CF-46CD-9586-FE891237AB8A}   ComponentServicesExtensionSnapin Class
{e0142b6f-a79d-451a-91a9-37e83ab696ec}   Fingerprint Enrollment UX
{E018945B-AA86-4008-9BD4-6777A1E40C11}
{e019c036-162f-4f57-a5bc-850e313210b7}   EAPHost Identity UI class
{E031F9E8-A35A-45EA-B263-F85FDED0D539}   Package State Setting Handler
{E0393303-90D4-4A97-AB71-E9B671EE2729}   VDS ProxyStub
{E03E85B0-7BE3-4000-BA98-6C13DE9FA486}   ConditionFactory Class
{E0519C57-3F89-4640-A63B-EF66268B52D9}
{e07dfaca-e658-4ce5-89b2-05bbbf75e708}   Sort-by Column Explorer Command
{e084f594-a1de-4038-b8d1-6c3c5fc3617c}   CLSID_HostedWindowFactory
{e0936539-81db-4574-b9f8-34fd0bff6f2e}   WinMDE RTSP SINK ACTIVATE
{E0BA3BF5-25EF-459F-9EE0-855FD3666692}   Corp Device Admin Helper
{E0BBDE88-67BA-4A0A-A452-86EF70F69FFE}   Modern Print Queue
{e0ca5340-4534-11cf-b952-00aa0051fe20}   HTML filter
{E0CBC546-8950-43DD-99A9-A418DB7DD0B5}   Could Not Connect Page Class
{e0ec8de2-d4e2-4e48-93ab-edcddbbcf7eb}   PSFactoryBuffer
{E0FA581D-2188-11D2-A739-00C04FA377A1}   Provider Binder for DS OLE DB Provider
{E10A508F-1699-40ba-A0DD-9DEB2D4DCAC3}
{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}   PSIProfileNotify
{E1150CE9-5BD4-4044-8FE9-98CF40137A41}   AudioProcessor Class
{E11685D3-11AF-4E03-9E55-895445C87F48}   Windows.ApplicationModel.LockScreen
{e126b7dd-1c3b-4821-b861-a6da9ce6f096}   ImeCommonAPIClassFactory_JPN_Desktop_V1
Class
{E137B0D0-7A93-11D2-8CEA-00A0C9441E20}   DxtJpegPP Class
{E13B6686-3F39-11D0-96F6-00A0C9191601}   DiskManagement.SnapIn
```

Page 110

SOFTWARE OUTPUT.txt
{E13B6688-3F39-11D0-96F6-00A0C9191601}  DiskManagement.DataObject
{E13B9A7F-EC39-4E7F-9970-12F348C89FD0}  PSFactoryBuffer
{E13EF4E4-D2F2-11d0-9816-00C04FD91972}  Menu Site
{E1553E07-5939-4CFD-BE24-3BCEBA2F148C}  Proxy CLSID
{e1625daf-d7c8-474b-b5c0-1525431d462c}  Explorer Setting Handler
{E164F996-FF93-4675-BDD8-6C47AB0B86B1}  SpHwVAEngine Class
{E16C0593-128F-11D1-97E4-00C04FB9618A}  Simple File-based Log
{E16C0594-128F-11D1-97E4-00C04FB9618A}  ARIES Log Recovery Engine
{E1779AD4-B31D-46be-BFA3-C1677A0A2851}  NarratorPane Class
{e1790c6b-8727-4598-bad3-6ba88a49c25d}  Miracast Connection Registrar class
{E18AF75A-08AF-11D3-B64A-00C04F79498E}  Custom Composition Segment from Legacy
Analog Tv Tuner Device Segment to Standard Video Renderer Device Segment
{E19AF835-9413-48A3-BDCC-28BA0286E348}  Microsoft Account UserIdKey Manager
{E19FF627-4C38-406D-9B4A-7973E0F539BA}  Playback Manager
{E1A6AFD2-7F54-4FD9-BF1D-F075EC94BB3F}  Keyboard AudioFeedback Class
{E1BA41AD-4A1D-418F-AABA-3D1196B423D3}  SDChangeObj Class
{E1BA88BA-7A83-421A-A05D-71F96C3FFFD0}  Windows.Devices.PointOfService
{E1C5D730-7E97-4D8A-9E42-BBAE87C2059F}  DeviceManager Class
{E1DE74AD-C368-4104-ADB1-57D00577247A}  WLAN Media Manager
{E1F1A0B8-BEEE-490D-BA7C-066C40B5E2B9}  Microsoft DTV-DVD Audio Decoder
{E1F5AA5B-065C-4E29-B454-C1BBFE0819D2}  Microsoft Account Credential Manager
{E2085F28-FEB7-404A-B8E7-E659BDEAAA02}  UPnPDeviceFinder Class
{E20870E2-3AD1-4b64-87BE-5AD5F17A53F0}  rtf persistent handler for mapi email
{E211B736-43FD-11D1-9EFB-0000F8757FCD}
{e2183960-9d58-4e9c-878a-4acc06ca564a}  Microsoft DocProp Custom Draw Multi-Value
Property Control
{e22ad333-b25f-460c-83d0-0581107395c9}  UIAutomation8 Client Central Class
{e22b3065-b83a-4ffd-9b08-9e73841a442f}  Content Snippet Builder
{E230022C-8258-41a4-AFF4-A917FE75C58B}  NarratorExpandCollapsePattern Class
{E23A07D1-1E89-4B22-8411-051B40A0A357}  Task Scheduler WMIv2 Provider
{E23B1CED-5E47-4FDB-AF66-B20370261B5E}  PimcManager Class
{E23CE3EB-5608-4E83-BCEF-27B1987E51D7}
{e2403e98-663b-4df6-b234-687789db8560}  RTF Filter
{E2448508-95DA-4205-9A27-7EC81E723B1A}  SBE2 Sink
{E2510970-F137-11CE-8B67-00AA00A3F1A6}  AVI mux
{e2550429-5df2-48cd-9ea3-26ff682d8a17}  Sort Descending Explorer Command
{E25E3D72-2E16-435D-88FC-27475DA85152}  WUDFClassExt
{E26B366D-F998-43ce-836F-CB6D904432B0}  RealTimeStylus Class
{E2765AC3-564C-40F9-AC12-CD393FBAAB0F}  Ribbon Share With Verb
{E296669F-B787-4A34-B23D-56F0AF1D450B}  WiFiCSP
{E2A4E630-7AD8-44f0-B6EE-D36EA4C6EB94}  Network Diagnostics Client Interface
Wrapper
{E2AD2F90-AC32-4DF6-B47A-61458E559320}  DSC PROXY
{E2AE5372-5D40-11D2-960E-00C04F8EE628}  SpNotifyTranslator Class
{e2b07466-5250-4fc2-8949-46bf91f8cad0}
{E2B71183-B72F-496A-8F5A-F1AC0D331471}  Device Pairing Config Proxy
{e2bf9676-5f8f-435c-97eb-11607a5bedf7}  Ribbon Modern Share Verb
{E2CBCB87-9C07-4523-A78F-061499C83987}  WMI instrumentation:
Win32_VolumeChangeEvent
{E2E5A310-ECED-444F-81D7-ACCA6AC8A1A8}  Win32_TpmProvider Class
{E2E760C5-BF0D-4241-BFD6-6D0AAB648AC9}  IE WS Change Notify
{E2E7934B-DCE5-43C4-9576-7FE4F75E7480}  Date and Time Control Panel
{E2E7969E-7186-4FE5-AAC9-1D9071AAFE4E}
Windows.Devices.Background.DeviceServicingDetails Factory
{e2eb4ca4-c96e-4da4-94b1-673c8334a5bb}  Shell Oplock Provider
{E2F33E30-B587-4f08-BF1A-F28D0F41000A}  Search Option Compressed Command
{E2F7A62A-862B-40AE-BBC2-5C0CA9A5B7E1}  ActivateAudioInterfaceWorker class
{e2fb4720-f45f-4a3c-8cb2-2060e12425c3}  MF AVI Property Handler
{E2FE048A-318B-4c79-A934-95AF2BCADEAC}  History command
{E302CB55-5F9D-41A3-9EF3-61827FB8B46D}  PSFactoryBuffer
{E30629D1-27E5-11CE-875D-00608CB78066}  Audio Renderer
{E30629D2-27E5-11CE-875D-00608CB78066}  Audio Capture Filter
{e317d729-81b0-4257-926b-b8de5f3b0288}  Share Platform Core
Page 111

SOFTWARE OUTPUT.txt

```
{E31A5806-8FD2-48EC-A132-7C1E614AC5B1}  Collection Staging State
{E31E87C4-86EA-4940-9B8A-5BD5D179A737}  RevealTrans
{E3250274-3AE3-472D-AA33-7BC11F195BAC}  CMCellularEntriesNodeProcessor
{e345f35f-9397-435c-8f95-4e922c26259e}  CLSID_StartMenuPathCompleteProviderFolder
{E3633C03-DF7A-41E0-B903-CC349A05E021}  PSFactoryBuffer
{E3784839-6BD5-4702-A7B0-59C7592FB7B8}  CSyncMLDPU
{E37A73F8-FB01-43dc-914E-AAEE76095AB9}  WTVFile Property Handler
{E37E2028-CE1A-4f42-AF05-6CEABC4E5D75}  Shell Icon Handler for Application
References
{E37EF07F-8266-448B-8059-C2B35BAFE0CF}  SnapinState Class
{E388F56A-D03B-4A08-ADC3-E44CA937AD91}  EdgeUI Device Manager
{e3a4e5ca-55b2-4a06-b1ab-8fbecc7bca4b}  Authentication UI Terminal Services Bump
Dialog
{E3A9BD50-51AE-410f-9706-0BA0D68B9A94}  Scavenged Files Cleanup
{E3C22B30-8502-4B2F-9133-559674587E51}  PSFactoryBuffer
{E3D5D93C-1663-4A78-A1A7-22375DFEBAEE}  InkTransform Class
{E3E1D967-0829-48AC-B3AD-C5AE4CA171C4}  SQLXMLX.1
{e3e478d6-a2f2-4791-89a3-21f5c78dc3ec}  File enumerator helper
{E410F8AE-00A1-4A1B-8247-924705718354}  State and invocation of verb commands
exposed by CommandFolder
{E413D040-6788-4C22-957E-175D1C513A34}  Sync Center Conflict Delegate Folder
{E4206432-01A1-4BEE-B3E1-3702C8EDC574}  Line 21 Decoder 2
{E423AF7C-FC2D-11d2-B126-00805FC73204}  RemoteHelper Class
{E4288337-873B-11D1-BAA0-00AA00BBB8C0}  CHS Language model
{E429B25A-E5D3-4D1F-9BE3-0C608477E3A1}  Table Driven Text Input Processor
{E436EBB1-524F-11CE-9F53-0020AF0BA770}  System Clock
{E436EBB2-524F-11CE-9F53-0020AF0BA770}  Filter Mapper
{E436EBB3-524F-11CE-9F53-0020AF0BA770}  Filter Graph
{E436EBB5-524F-11CE-9F53-0020AF0BA770}  File Source (Async.)
{E436EBB6-524F-11CE-9F53-0020AF0BA770}  File Source (URL)
{E436EBB7-524F-11CE-9F53-0020AF0BA770}  IPersistMoniker Plug In Distributor
{E436EBB8-524F-11CE-9F53-0020AF0BA770}  Filter Graph no thread
{E444E1B9-502C-44f9-B714-30DA330D0E8E}  WorkspacePolicyProcessor Class
{E44E5D18-0652-4508-A4E2-8A090067BCB0}  Default Programs command object for Start
menu
{e44e9428-bdbc-4987-a099-40dc8fd255e7}  Execute Unknown
{e4544aba-62bf-4c54-aab2-ec246342626c}  CloudExperienceHost Create System Object
Task
{e46787a1-4629-4423-a693-be1f003b2742}  MF WAV Property Handler
{E46C6E1E-8ADE-4EDD-AFAA-446D1999911B}
{E474E05A-AB65-4f6a-827C-218B1BAAF31F}  MF Video Mixer
{E4785230-0E43-47DC-826A-07DBC3AA63D8}  DsmControl Class
{e4796550-df61-448b-9193-13fc1341b163}  Property Store
{E48B2549-D510-4A76-8A5F-FC126A6215F0}  CLSID_AntiPhishingBrowserSolution
{E48EDA45-43C6-48e0-9323-A7B2067D9CD5}  File Change Tracker Internal
{E49741E9-93A8-4AB1-8E96-BF4482282E9C}  System Monitor Appearance Properties
{E4979309-7A32-495E-8A92-7B014AAD4961}  VMR ImageSync 9
{E49F7E50-C070-11DF-AC23-18A90531A85A}  PSFactoryBuffer
{E4BCAC13-7F99-4908-9A8E-74E3BF24B6E1}  DirectSoundCapture 8.0 Object
{E4C1D9A2-CBF7-48BD-9A69-34A55E0D8941}  DirectPlay8 NAT Resolver Object
{E4D5B02C-82A9-4363-BD02-8BA595200BCF}  HomeGroup Join Command
{e4e55606-2ffb-4558-a601-7693efc5481c}  WinMDE NETCHANNEL ACTIVATE
{E4E915A9-8344-4F88-9326-2ADC071D4FF6}
{E524CB3D-29DF-49AD-BF4E-AFF32F8551AC}
{E52C9A25-F3E8-49E4-BAA7-FAD0EF620129}
{e53cd6ee-5c5c-4701-9ff2-c204bfed819d}  LicenseManagerFactory
{E54CDFAF-2381-4cad-AB99-F38517127D5C}  MF MP3 Sink Class Factory
{E54E4714-22AE-40c5-BB24-F839845C7C98}
{E569BDE7-A8DC-47F3-893F-FD2B31B3EEFD}  Browser Application State
{E573236F-55B1-4EDA-81EA-9F65DB0290D3}
{e57401ab-d6b3-4deb-979e-f082052dd374}
{E579AB5F-1CC4-44b4-BED9-DE0991FF0623}  VSSCoordinator Class
{e5899c7c-0fc7-499e-a262-174fd692dc9f}  CCAPIProvider
```

Page 112

SOFTWARE OUTPUT.txt

```
{E593941A-F61C-49C3-85F1-D00EBF0D4EB2}  ChxAdvancedDS
{E598560B-28D5-46aa-A14A-8A3BEA34B576}  Windows Photo Viewer Video Verbs
{e5b35059-a1be-4977-9bee-5c44226340f7}  PSFactoryBuffer
{E5B4EAA0-B2CA-11CE-8D2B-0000E202599C}  MPEG Video Decoder Property Page
{E5B5B938-52A0-4B37-8659-24EB5165B9A0}  Microsoft Direct Access WMI Provider
{E5B8E079-EE6D-4E33-A438-C87F2E959254}  Location Class
{E5CA59F5-57C4-4DD8-9BD6-1DEEEDD27AF4}  Microsoft InkEdit Control
{e60687f7-01a1-40aa-86ac-db1cbf673334}  SUSInternal Class 1.0
{E61B54C9-1261-4929-8A64-4DEFAF49191B}  RetailInfo.ProxyStub
{E61BF828-5E63-4287-BEF1-60B1A4FDE0E3}  Work Folders Context Menu Handler
{E6290C32-443A-4529-AEC3-320ADF0F9622}  Favorite Shortcuts Setting Handler
{E6335F02-80B7-4DC4-ADFA-DFE7210D20D5}  Microsoft MPEG-2 Video Encoder MFT
{E63DE750-3BD7-4BE5-9C84-6B4281988C44}  Windows Search Scope Rule
{E64164EB-1AE0-4C50-BAEF-A413C2B3A4BC}  Microsoft 3MF Shell Thumbnail Handler
{E6442437-6C68-4f52-94DD-2CFED267EFB9}  CLSID_TrayDesktopBand
{e657ebe3-9854-4ee6-8d2a-2d885fc6e1db}  Composite Windows Push Notification
Polling Url Handler
{E68d2B3E-192D-448E-827E-239082D74DC6}  Windows.Networking.UX.ProxyStub
{E69FD98D-7EBE-4C01-BFED-67B4E4616A49}  Browser Thread Handshake
{E6B1A103-277A-4D64-ABD0-90151F9CAB82}  Input Personalization Setting Monitor
{E6E46E80-CA08-49DD-93E8-A2DDB88FD14B}  LayerManager Class
{E6E73D20-0C8A-11d2-A484-00C04F8EFB69}  CrZigzag
{E6EE9AAC-F76B-4947-8260-A9F136138E11}  IE Shell Band Site Menu
{e6f721c1-034a-48b6-96dd-ce36ced74a03}  Windows.Media.Ocr PSFactory
{E70C92A9-4BFD-11d1-8A95-00C04FB951F3}  CLSID_StoreNamespace
{E71B4063-3E59-11D2-952A-00C04FA34F05}  Shadow
{E73A797B-24CE-424A-AD4F-48E98B1E95B8}
Windows.Internal.Security.Authentication.Web.CTokenBrokerMessageBroker
{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435}  CCertProvider
{e755468c-02f5-4d96-8487-3be68ffe633a}  Elevated Object Factory Server Manager
{E756C791-2001-4de5-83C7-DE61D88831D0}  {E756C791-2001-4de5-83C7-DE61D88831D0}
{e760e244-abb3-4c3c-b925-0781c8ceb46c}
{E77026B0-B97F-4cbb-B7FB-F4F03AD69F11}  Tuning Model Xml Serialization Utility
{E7772804-3287-418E-9072-CF2B47238981}
{E77CC89B-7401-4c04-8CED-149DB35ADD04}  WindowsParentalControls Class
{E77E1B8B-ECF3-4af0-8B5E-EB13739D5344}
{e79167d7-1b85-4d78-b603-798e0e1a4c67}  MF Media Source Activate
{e7a7a3e2-c61b-4f1f-ab41-e929dd7fa60d}  PSFactoryBuffer
{E7B0F685-6247-4E7D-823E-06DEE79A8AA9}  RASGCW Non UI Class
{E7B2FB72-D728-49B3-A5F2-18EBF5F1349E}  PSFactoryBuffer
{E7B3C0E0-FB47-49F6-A66B-8A7C2E4E7B9C}  CoPrintIsolationSessionHost Class
{E7D35CFA-348B-485E-B524-252725D697CA}  PSFactoryBuffer
{E7DE514C-BBBC-41D4-8838-4BB0FE21229A}  Activation Error Popup Factory
{E7E4BC40-E76A-11CE-A9BB-00AA004AE837}  Shell DocObject Viewer
{E7E6A098-87CE-420D-91AE-413312AC8FA6}  Windows Firewall Helper Class
{E7E79A30-4F2C-4FAB-8D00-394F2D6BBEBE}
{E7E977EF-BE01-447B-8108-B9C84F45B946}  PSFactoryBuffer
{e7ed314f-2816-4c26-aeb5-54a34d02404c}  KernelCeipCustomHandler
{E7F328B1-6095-41B0-94B7-3DD278EADAA1}  Microsoft.WINDOWS.SQLLITE.Param.4.0
{E800E945-780D-48D3-89E7-D822EA18F0A2}  PSFactoryBuffer
{E801D4C9-C485-46AF-B839-7A16D4895182}  Windows.Gaming.XboxLive.Storage
{E810CEE7-6E51-4cb0-AA3A-0B985B70DAF7}  StrokeBuilder Class
{E8167EE2-AB45-4BAA-BD03-12590436D789}  CLSID_COE7Import
{e82a2d71-5b2f-43a0-97b8-81be15854de8}  ShellLink for Application References
{E838B72C-83C9-4a08-8DD1-144CB14616F1}  Setting Unit Resolver
{E846F0A0-D367-11D1-8286-00A0C9231C29}
{E847030C-BBBA-4657-AF6D-484AA42BF1FE}  PSFactoryBuffer
{E88DCCE0-B7B3-11d1-A9F0-00AA0060FA31}  CompressedFolder
{E8C40B98-FCF5-4047-86DA-11A11590CB98}  Language Setting Handler
{e8e4dbb7-bfa1-4a0c-a168-b0568d4654e2}  Turn Off Preview Panes Explorer Command
{E8E9D2D1-130A-4460-98BB-48C9A6F280B9}  NarratorScrollPattern Class
{E8FD5270-2AFB-4345-A75B-C8F5C3A412A3}  PSFactoryBuffer
{e916b6b2-22bd-4afc-b337-d3d9fb27670e}  AudioCopy Class
```

Page 113

SOFTWARE OUTPUT.txt

```
{E9218AE7-9E91-11D1-BF60-0080C7846BC0}  SdoMachine Class
{E9225296-C759-11d1-A02B-00C04FB6809F}  DispatchMapper Class
{e9309678-18b4-414b-ba7a-2c9a7bcf9684}  OOBE Broker Manager
{E9495B87-D950-4ab5-87A5-FF6D70BF3E90}  Security Center
{E95186C7-7D80-4311-843D-0702CBC8B1E4}  Remove Device Elevated Handler
{E9571AB2-AD92-4ec6-8924-4E5AD33790F5}  Permanent delete command
{E96767E0-7EAA-45E1-8E7D-64414AFF281A}  File Prop Sheet Page Helper
{E96F5460-09CE-4f46-88B1-F4B6B4A8E252}  Windows Media Player Transcode Files Cache
Cleanup Handler
{e9711a2f-350f-4ec1-8ebd-21245a8b9376}  Navigation Pane Show Libraries Command
{E974D26D-3D9B-4D47-88CC-3872F2DC3585}  XPS Object Factory
{E979DAD9-25E8-45D7-AB42-43FB7B9F38CC}  SpW3CSemanticInterpretation Class
{E97D552D-9AE9-46AA-9151-D2DA4BBB5E96}  TaskCompletionClient
{E98B8DC5-72E3-48E4-A4BC-9393F3EA0DA5}  PolicyManager.ProxyStubFactory
{e9970fa4-b6aa-11d9-b032-000d56c25c27}  IAS SDO Helper Class
{E9A6AB1B-0C9C-44AC-966E-560C2771D1E8}  DrawAttrsXP Class
{E9BE10DC-8454-4FC5-A70F-C2E0F6323BC1}  CLSID_MIMEBinHexDecoder
{E9F4EBAB-D97B-463e-A2B1-C54EE3F9414D}  Net Scheme Handler
{EA022610-0748-4c24-B229-6C507EBDFDBB}  CLSID_HomeGroupCtrlServer
{EA15B5D3-1E8F-482f-B127-66764C6A762E}  Content Tile Setting Handler
{ea297d29-fc9f-41ef-a2e0-666891b01c6e}  CloudExperienceHost Elevation Broker
Manager
{EA2C6B24-C590-457B-BAC8-4A0F9B13B5B8}  User Account Control Settings
{EA30C654-C62C-441f-AC00-95F9A196782C}  GestureRecognizer Class
{EA502722-A23D-11D1-A7D3-0000F87571E3}  Group Policy Object
{EA678830-235D-11d2-A8B6-0000F8084F96}  CLSID_IPropPatchRequest
{ea72d00e-4960-42fa-ba92-7792a7944c1d}  Run as different user context menu handler
{ea8b451c-5a19-49cf-bc5e-98accca49ef3}  Library Factory
{EA92B647-F9C1-48ED-A0FF-433E54FF0D73}
Windows.Web.Http.Diagnostics.ProxyStubFactory
{EAB16C5D-EED1-4E95-868B-0FBA1B42C092}  Windows Store Remote Desktop Client
Control - version 1
{EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}  Microsoft Web Browser Version 1
{EAC8A024-21E2-4523-AD73-A71A0AA2F56A}  WbemQuery
{EAE826D3-ECB5-49ff-BC55-7B318E78C6DD}  Dot3BalloonHandler Class
{eb124705-128b-40d4-8dd8-d93ed12589a4}  WPL property store
{EB36A2D2-BA9E-457F-8023-66EE08D4D955}  SpGramCompBackEnd Class
{eb4d075a-65c0-476b-956c-c605eade03f7}  DemuxRender
{EB56EAE8-BA51-11d2-B121-00805FC73204}
{EB6B4457-F013-4E5A-9B05-1D44E4D6FAEB}  HomeGroup Sharing Hosted Listener
{EB87E1BD-3233-11D2-AEC9-00C04FB68820}  WbemStatusCode
{EB9D0A19-E64D-4C85-A6A1-45EFAB463E6F}  PrintNotificationEventDetails
{EBB08C45-6C4A-4FDC-AE53-4EB8C4C7DB8E}  TF_LangBarMgr
{EBB236B1-F57F-480D-9DE9-B15A87298EEC}  Retail Demo User Agent
{EBF00FCB-0769-4b81-9BEC-6C05514111AA}  FamilySafety.WebSync
{EBF024CD-CF8A-4D2A-9132-43CFD49ACBB3}  Windows Connected Search Paths Provider
{EBFE7BA0-628D-11D2-AE0F-006097B01411}  DirectPlay8 WSock TCPIP Provider Object
{EC00BA63-C73A-4679-AC8D-69366C766989}  SBE Stats - receiver side
{ec05b81f-ec57-47c9-a6ce-eebc9b35861b}  Override Scaling
{EC0AE07D-6A4C-49a4-8A40-F130C525D7D9}  AudioKSHWEndpoint Class
{ec4db96f-6872-4903-a448-6dffc454ae6d}  PlayToDevice
{ec57976f-0796-42b5-a699-6a24933a48bc}  Casting protocol App Manager and Launcher
class
{EC8A7A18-FE68-403f-9625-CF63026F1BB4}  DevicePicker ProxyStub
{ec8f67f0-a2de-4868-98e6-eaad214bcdc6}  ChxProxyDS
{EC9BA17D-60B5-462B-A6D8-14B89057E22A}  Barn
{ecabafaa-7f19-11d2-978e-0000f8757e2a}  Activity Property Unmarshal Class
{ecabafab-7f19-11d2-978e-0000f8757e2a}  SecurityEnvoy
{ecabafac-7f19-11d2-978e-0000f8757e2a}  Transaction Property Unmarshal Class
{ecabafad-7f19-11d2-978e-0000f8757e2a}  NonRootTransactionEnvoy
{ecabafae-7f19-11d2-978e-0000f8757e2a}  sca Class
{ecabafaf-7f19-11d2-978e-0000f8757e2a}  ClassFactory Activator Class
{ecabafb0-7f19-11d2-978e-0000f8757e2a}  obja Class
```

Page 114

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {ecabafb1-7f19-11d2-978e-0000f8757e2a} | stapa Class |
| {ecabafb2-7f19-11d2-978e-0000f8757e2a} | vca Class |
| {ecabafb3-7f19-11d2-978e-0000f8757e2a} | User Context Object |
| {ecabafb4-7f19-11d2-978e-0000f8757e2a} | User Context Properties Association Object |
| {ecabafb5-7f19-11d2-978e-0000f8757e2a} | PoolMgr Class |
| {ecabafb6-7f19-11d2-978e-0000f8757e2a} | Object Pool Activator Class |
| {ecabafb7-7f19-11d2-978e-0000f8757e2a} | Contruction Activator Class |
| {ecabafb9-7f19-11d2-978e-0000f8757e2a} | COM+ Instance Tracking Component |
| {ecabafbc-7f19-11d2-978e-0000f8757e2a} | COM+ Event Notification Server |
| {ecabafc0-7f19-11d2-978e-0000f8757e2a} | cfw Class |
| {ecabafc2-7f19-11d2-978e-0000f8757e2a} | Queued Components Recorder |
| {ecabafc3-7f19-11d2-978e-0000f8757e2a} | QC Listener Class |
| {ecabafc4-7f19-11d2-978e-0000f8757e2a} | Queued Components Player |
| {ecabafc6-7f19-11d2-978e-0000f8757e2a} | New Moniker |
| {ecabafc7-7f19-11d2-978e-0000f8757e2a} | Queue Moniker |
| {ecabafc9-7f19-11d2-978e-0000f8757e2a} | QC Queue Administration Class |
| {ecabafca-7f19-11d2-978e-0000f8757e2a} | COM+ QC Dead Letter Queue Listener Starter |
| {ecabafcb-7f19-11d2-978e-0000f8757e2a} | QC Marshal Interceptor Class |
| {ecabafcc-7f19-11d2-978e-0000f8757e2a} | Partition Property Unmarshal Class |
| {ecabafcd-7f19-11d2-978e-0000f8757e2a} | Tracking Info Collection Unmarshal Class |
| {ecabafce-7f19-11d2-978e-0000f8757e2a} | Tracking Info Object Unmarshal Class |
| {ecabafcf-7f19-11d2-978e-0000f8757e2a} | EventRegistrar Class |
| {ecabafd0-7f19-11d2-978e-0000f8757e2a} | Soap Activator Class |
| {ecabafd3-7f19-11d2-978e-0000f8757e2a} | ObjWrapperMarshaler Class |
| {ecabb0a8-7f19-11d2-978e-0000f8757e2a} | COM+ Services GetSecurityCallContext |
| {ecabb0aa-7f19-11d2-978e-0000f8757e2a} | Byot Server Extended Object |
| {ecabb0ab-7f19-11d2-978e-0000f8757e2a} | MTSEvents Class |
| {ecabb0ac-7f19-11d2-978e-0000f8757e2a} | MTSLocator Class |
| {ecabb0bd-7f19-11d2-978e-0000f8757e2a} | CrmClerk Class |
| {ecabb0be-7f19-11d2-978e-0000f8757e2a} | CrmRecoveryClerk Class |
| {ecabb0bf-7f19-11d2-978e-0000f8757e2a} | MessageMover Class |
| {ecabb0c0-7f19-11d2-978e-0000f8757e2a} | DispenserManager |
| {ECABB0C3-7F19-11D2-978E-0000F8757E2A} | ComEvents.ComServiceEvents |
| {ecabb0c4-7f19-11d2-978e-0000f8757e2a} | Debug Dump Server |
| {ecabb0c5-7f19-11d2-978e-0000f8757e2a} | Partition Moniker |
| {ECABB0C6-7F19-11D2-978E-0000F8757E2A} | ComEvents.ComSystemAppEventData |
| {ecabb0c7-7f19-11d2-978e-0000f8757e2a} | SOAP Moniker |
| {ecabb0c8-7f19-11d2-978e-0000f8757e2a} | CServiceConfig Class |
| {ECABB0C9-7F19-11D2-978E-0000F8757E2A} | |
| {ECABB0CA-7F19-11D2-978E-0000F8757E2A} | |
| {ECB17B16-24AF-41E2-864C-34FE5427FF37} | |
| {ECC82A10-B731-3A01-8A17-AC0DDD7666CF} | System.Security.HostProtectionException |
| {ECCDF543-45CC-11CE-B9BF-0080C87CDBA6} | DfsShell Class |
| {ECD32AEA-746F-4dcb-BF68-082757FAFF18} | DynamicRenderer Class |
| {ECD4FC4D-521C-11D0-B792-00A0C90312E1} | Shell Rebar BandSite |
| {ECD4FC4E-521C-11D0-B792-00A0C90312E1} | Shell Band Site Menu |
| {ECD4FC4F-521C-11D0-B792-00A0C90312E1} | Menu Desk Bar |
| {ECF03A32-103D-11d2-854D-006008059367} | MyDocs Drop Target |
| {ecf5bf46-e3b6-449a-b56b-43f58f867814} | Identity Store Profile Notification |
| {ed1d0fdf-4414-470a-a56d-cfb68623fc58} | Play with Windows Media Player |
| {ED228FDF-9EA8-4870-83b1-96b02CFE0D52} | Games Explorer |
| {ED368BA2-23B5-4FC1-9143-AC6A71ECF549} | AppListEntryClientProxy |
| {ED3AF319-8B2B-455F-91A2-AC3B76111C43} | Device Tile Builder |
| {ED43BB3C-09E9-498a-9DF6-2177244C6DB4} | FhConfigMgr Class |
| {ED4B1828-CD88-460F-AEFF-3D63FC8BBF68} | Microsoft Domain Name System (DNS) Client WMIv2 Provider |
| {ed50fc29-b964-48a9-afb3-15ebb9b97f36} | printhood delegate folder |
| {ed6ae9cf-ad35-46b7-ac30-3f8b9eb5349f} | TryHarderFactory |
| {ed72f0d2-b701-4c53-adc3-f2fb59946dd8} | ProtectedModeAPI |
| {ED7BA470-8E54-465E-825C-99712043E01C} | All Tasks |
| {ED822C8C-D6BE-4301-A631-0E1416BAD28F} | |
| {ED8C108E-4349-11D2-91A4-00C04F7969E8} | XML HTTP Request |
| {ED8C22CA-7722-464A-A522-7967ABF63C35} | HomeGroup Sharing Command |

Page 115

SOFTWARE OUTPUT.txt

```
{ED999FF5-223A-4052-8ECE-0B10C8DBAA39}   ActualWbemUnauthenticatedLocator Class
{ed9d80b9-d157-457b-9192-0e7280313bf0}   Compressed (zipped) Folder DropHandler
{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}   Share Manager
{EDB9987A-FFF5-4bd2-8B05-2865F3EC621D}   Image Sanitization Validator
{edc3a8b5-2e25-466a-a1ad-21e2f19414ac}   MF AC3 Property Handler
{EDC978D6-4D53-4b2f-A265-5805674BE568}   StreamBackedFolder
{EDD36029-D753-4862-AA5B-5BCCAD2A4D29}   Property Store Collection
{edd749de-2ef1-4a80-98d1-81f20e6df58e}   PLAP Logon Provider Filter
{EDEA4743-46D4-4C14-B358-64FD126052EC}   State and invocation of verb commands
implemented by IContextMenuCB
{EDF6970E-4557-4BC5-86C2-C7E52A06B27F}   PSFactoryBuffer
{EE09B103-97E0-11CF-978F-00A02463E06F}   Scripting.Dictionary
{EE0BDDFA-8373-4cc4-85D8-0618E453187C}   IE History Search Protocol Handler
{EE14E412-4988-458C-B863-76E3C1BF71C2}   OOBE HidMousePairing Wizard Page
{ee20eeba-df64-4a4e-b7bb-2d1c6b2dfcc1}   UnPin From Frequent Command
{EE24A2C3-3AA2-33DA-8731-A4FCC1105813}   System.Security.Policy.GacInstalled
{EE366069-1832-420F-B381-0479AD066F19}
{EE4DA6A4-8C52-4a63-BBB8-97C93D7E1B6C}   APPLICATION__X_MS_WMD Moniker Class
{EE5799D0-070A-49EE-8476-6A02E46E9FDD}   OOBE Localization Page
{EE8E4870-A889-4DC4-969F-F38F707F4AC2}   CTaskCondition
{eea0c191-dda8-4656-8fc4-72bdedba8a78}   Library Property Store
{EEBD2F15-87EE-4f93-856F-6AD7E31787B3}   CPartitionSetContextMenu Class
{EEC6993A-B3FD-11D2-A916-00C04FB98638}   Microsoft USB PID Class Driver
{eec97550-47a9-11cf-b952-00aa0051fe20}   HTML File persistent handler
{EF011F79-4000-406D-87AF-BFFB3FC39D57}   DirectSoundCompressorDMO
{EF114C90-CD1D-484E-96E5-09CFAF912A21}   DirectSoundDistortionDMO
{EF19FBF6-0212-4463-8B3E-14E1318DC616}   MediaObjectInfo
{ef1c0450-0b48-4384-94ae-d1cb35641f86}   Categorizer Factory
{EF30258D-9897-45CD-A760-FE5C195CB00E}   Setting Sync Settings
{EF3E932C-D40B-4F51-8CCF-3F98F1B29D5D}   DirectSoundEchoDMO
{EF411752-3736-4CB4-9C8C-8EF4CCB58EFE}   SpObjectToken Class
{ef43ecfe-2ab9-4632-bf21-58909dd177f0}   Folder Customization Tab
{EF4D1E1A-1C87-4AA8-8934-E68E4367468D}   WebCheck
{EF544DC6-8DD8-4D8E-B867-BC728AC2B6D7}   DevicePackagesInfo CSP
{EF5C5336-1AF1-42E8-8AAD-FC2453B765DE}   InkRecognizerGuide Class
{ef5db4c2-9312-422c-9152-411cd9c4dd84}   Provides access to a portable device
service using IPortableDeviceService
{ef636390-f343-11d0-9477-00c04fd36226}   OLE DB Rowset Proxy
{ef636391-f343-11d0-9477-00c04fd36226}   OLE DB Rowset Server
{ef636392-f343-11d0-9477-00c04fd36226}   OLE DB Row Proxy
{ef636393-f343-11d0-9477-00c04fd36226}   OLE DB Row Server
{EF7DEED8-27D0-42DC-B135-664EEFC69F52}   Windows.Web.Http.ProxyStubFactory
{ef7e0655-7888-4960-b0e5-730846e03492}   psfactorybuffer
{EF7F04A5-461B-4E32-840D-5841AB00713C}   Lifetime Manager
{EF8AD2D1-AE36-11D1-B2D2-006097DF8C11}   Global Folder Settings
{EF985E71-D5C7-42D4-BA4D-2D073E2E96F4}   DirectSoundI3DL2ReverbDMO
{EFA24E64-B078-11D0-89E4-00C04FC9E26E}
{EFA53AE9-2604-4a34-9E67-674842B4CB35}   EnumerableObjectCollection Marshal By
Value
{EFA97F08-EE06-42EC-AAAF-F8CB106247A2}   Appx File Streaming Data Source Factory
Object
{EFB4A0CB-A01F-451C-B6B7-56F02F77D76F}   GenericRecognizer Class
{EFB92EFB-9236-4bd7-B60D-51D1C7D1C87A}   Framing Layer Helper Class
{EFCA3D92-DFD8-4672-A603-7420894BAD98}   DirectSoundFlangerDMO
{efce38d3-8914-4674-a7df-ae1b3d654b8a}   MFCaptureEngine Class Factory
{EFDB73A6-192F-4944-979E-4153CC8E8715}   Microsoft.WINDOWS.SQLLITE.Error.4.0
{EFE3FA02-45D7-4920-BE96-53FA7F35B0E6}   BDA Tuning Model DVB Terrestrial 2 Locator
{EFE6208A-0A2C-49FA-8A01-3768B559B6DA}   MF AMRNB Media Source ByteStreamHandler
{EFE6629C-81F7-4281-BD91-C9D604A95AF6}   DirectSoundChorusDMO
{EFEA49A2-DDA5-429D-8F42-B23B92C4C347}   PSFactoryBuffer
{EFEB5035-1DA0-4B73-AFA2-68ED7A1D98E0}   RetailInfoSetterInternal
{F00006F2-44BC-44EF-808B-B26002A183C2}   DIAL Receiver Activation Plugin
{F00B4404-F8F1-11CE-A5B6-00AA00680C3F}   WBEM PerfMon Instance Provider
```

Page 116

SOFTWARE OUTPUT.txt

```
{F0152790-D56E-4445-850E-4F3117DB740C}  Remote Sessions CPL Extension
{F020E586-5264-11d1-A532-0000F8757D7E}
{F022A390-2F1E-44d2-AA0A-0FEB28AE6517}  DXP
{F02602C4-3C2A-473B-B35E-679A0076A4A6}  GenValObject Inner Class
{F0285374-DFF1-11D3-B433-00C04F8ECD78}  ConsolePower Class
{F0291081-E87C-4E07-97DA-A0A03761E586}  Drawing
{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}  Computers and Devices
{F04C3F9B-20B3-40E1-A824-3A41FE3D7931}  DSC Core Configuration Provider
{F04CC277-03A2-4277-96A9-77967471BDFF}  Sync Center Conflict Properties Extension
{F052299C-6DA4-40f0-BE0D-8BD02FAD080A}  OOBE ProtectPC Plugin
{f05cca50-64a6-47df-a4d1-ef4427ab32be}  Composite Windows Push Notification
Setting Handler
{F063A606-6748-4b89-82A0-3D19D94CE8D3}  SyncTaskHandler Class
{F074C547-461C-4146-B35A-F1F845AF413B}
{f079ec7c-11a4-4c33-87fa-090d19772fac}  PEAP Identity UI class
{F0820DE1-3969-4BA6-A090-E99687AE929B}  Windows.Devices.Midi
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}  Background Intelligent Transfer Control
Class 1.5
{F088DE73-BDD0-4E3C-81F8-6D32F4FE9D28}  Stretch
{F08C5AC2-E722-4116-ADB7-CE41B527994B}  Bluetooth Authentication Agent SSO
{F0A3A195-8D6A-4BC7-BD1F-3B2A2D5807CA}  LiveProviderRegistrar
{f0ae1542-f497-484b-a175-a20db09144ba}
{F0B1E31E-4FE1-49F5-84BC-4BA007655288}  Sync Settings Handler
{f0ce6592-5bce-41cc-bf2d-ec4f3f55e711}  CStorageItemPropertiesProxy
{F0DB4512-0E25-4A1F-A88B-8FF40351BFCD}  Switch Thumbnail Device Manager
{F1171280-BC35-45d1-8F53-8AB833267899}  DNS Helper Class
{F1184172-589C-4ECA-B2C8-F330C903A76F}  ClientCertificateInstall
{F1390A9A-A3F4-4E5D-9C5F-98F3BD8D935C}  Sync Setup Delegate Folder
{F1425A67-1545-44A2-AB59-8DF1020452D9}  Spell Checking Host Class
{F159A1A7-462A-4FF3-8E51-E518DC011268}  CFmIfsEngine Class
{F1759E97-0B98-49DA-8B38-372CD47DC97B}  Wireless Setting Handler
{F198A89A-5042-4294-ADF1-CB163E549798}  Win32_EncryptableVolumeProvider Class
{f1bd1079-9f01-4bdc-8036-f09b70095066}  psfactorybuffer
{F1E752C3-FD72-11D0-AEF6-00C04FB6DD2C}  DocConfig 1.0 Object
{F1EFACAA-08A1-461B-9D28-7AA8947889A0}
{f1f72421-6433-4de9-982d-c8dc12cb569c}  Oplock Handle Marshaller
{F20487CC-FC04-4B1E-863F-D9801796130B}  Sync Center Shell Service Object
(Internal)
{F20DA720-C02F-11CE-927B-0800095AE340}  Package
{F2102C37-90C3-450C-B3F6-92BE1693BDF2}  Windows Security Center ISV API
{f216b1bc-2310-49d6-930f-ae8837bda4b0}  CastLaunch
{F22F5E05-585C-4def-8523-6555CFBC0CB3}  CTocEntry
{f235ce7d-b143-4d4f-ad93-64e48d53a5fb}  CLSID_KnownAutoListManager
{f2468580-af8a-11d0-8212-00c04fc32c45}  AuStream Class
{F2472B49-5214-4D3A-A662-04F09250D694}  WlanDlgNonUIFinishPage Class
{F249C9EA-8DB4-43DC-B2BC-146A61D23D99}  Foreground Manager MUX
{f26a669a-bcbb-4e37-abf9-7325da15f931}  AutoPlayVerb
{f270c64a-ffb8-4ae4-85fe-3a75e5347966}  ADs Security Utility Object
{F2C2787D-95AB-40D4-942D-298F5F757874}  PSFactoryBuffer
{f2c3faae-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.OU
{F2C4CDB0-2714-42AD-A948-2ED958A322E3}  WorkspaceResTypeRegistry Class
{F2DDFC82-8F12-4CDD-B7DC-D4FE1425AA4D}  Sound Control Panel
{f2f84074-8bca-40bd-9159-e880f673dd3b}
{F2FC5C3B-FC71-452c-AB56-47BC0873E46D}  OOBE Region Plugin
{F31091EA-B0A8-11D6-B6FC-005056C00008}  CmiFactory Class
{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}  Microsoft WBEM New Event Subsystem
{F32063EA-DF0C-437D-BD5E-5E718683E4A3}  NarratorScrollItemPattern Class
{F324E4F9-8496-40b2-A1FF-9617C1C9AFFE}  Sync root manager
{F3252D7B-E51D-4B14-AA5E-8E3D4315F73C}  PSFactoryBuffer
{F32E8FA6-A99F-4E9B-AF78-C929EBB73589}  Action Execution Broker Class Factory
{F3364BA0-65B9-11CE-A9BA-00AA004AE837}  Shell File System Folder
{F3368374-CF19-11d0-B93D-00A0C90312e1}  OrderListExport
{f371728a-6052-4d47-827c-d039335dfe0a}  Mpeg4 Decoder DMO
```

Page 117

SOFTWARE OUTPUT.txt

```
{F375FDC3-9DB0-4927-A84A-FC1215B3570F}  SpWaveFormatEx Class
{F37AFD4F-E736-4980-8650-A486B1F2DF25}  windows_Search_OutlookToolbar
{F37C5810-4D3F-11d0-B4BF-00AA00BBB723}  Security Shell Extension
{F382DA49-9148-4a22-AF78-C378DFC32D02}  MS_InstalledGameProv Class
{F3BDFAD3-F276-49e9-9B17-C474F48F0764}  CQueryWinSAT Class
{F3C633A2-46C8-498E-8FBB-CC6F721BBCDE}
{f3cc4ca3-22c2-40ec-ac3c-89d8a43373b0}  Include the selected folder in a library.
{F3CCAE10-A927-4D4E-9138-4A513C4B10FA}  windows.Media.Import.ProxyStubFactory
{f3d06e7c-1e45-4a26-847e-f9fcdee59be0}  Copy as Path Menu
{F3D3F924-11FC-11D3-BB97-00C04F8EE6C0}  SpCFGEngine Class
{f407d01a-0bcb-4591-9bd6-ea4a71df0799}  CHT Language model
{f4086d4e-2e05-428b-92de-87d8d0bb4262}  Pnrp Helper Class
{F412BFA1-8035-472B-8185-F13B8C29CF21}  CommandGenerator Class
{F42F750A-64A8-4190-951D-C6F7EF4E4BA1}  EDP Notification Host
{F43E8166-162C-4B12-8C2B-510D21516082}  Microsoft NDIS VmSwitch Teaming WMI
Provider
{F440168E-A06A-4C25-B6EB-01705985E826}  Browser Favorites Setting Handler
{F4477AD6-6B3A-411b-9ECC-7CE89B665401}  CWapDPU
{f447b69e-1884-4a7e-8055-346f74d6edb3}  Resampler DMO
{F46316E4-FB1B-46eb-AEDF-9520BFBB916A}  Dynamic Storage Object
{F4655419-DAF2-42ab-9178-3B6AC903170C}  RNWF MSM Helper Class
{f4ba59cc-2506-45ae-84c8-78ea8d7f9b3e}  Compat Inventory WMI provider
{f4be747e-45c4-4701-90f1-d49d9ac30248}  PerfCenter Enabler
{F4D36777-EAED-4cc5-9FE7-827BE5190B20}  Microsoft Feeds Scheduler
{f4d8c39a-f43d-42b4-9bdf-4e48d3044ba0}  Name Resolution Policy
{F4E1E7F6-A035-41B3-9856-A3C3A1C4684F}  WCF/COM+ Integration Service Moniker 40
{f4e8bc67-9616-4a28-a332-cf27a5ca6736}  Size All Columns Explorer Command
{F5078F19-C551-11D3-89B9-0000F81FE221}  XML Parser
{F5078F27-C551-11D3-89B9-0000F81FE221}
{F5078F31-C551-11D3-89B9-0000F81FE221}  XML Parser 3.0
{F5078F32-C551-11D3-89B9-0000F81FE221}  XML DOM Document 3.0
{F5078F33-C551-11D3-89B9-0000F81FE221}  Free Threaded XML DOM Document 3.0
{F5078F34-C551-11D3-89B9-0000F81FE221}  XML Schema Cache 3.0
{F5078F35-C551-11D3-89B9-0000F81FE221}  XML HTTP 3.0
{F5078F36-C551-11D3-89B9-0000F81FE221}  XSL Template 3.0
{F5078F37-C551-11D3-89B9-0000F81FE221}
{F5078F39-C551-11D3-89B9-0000F81FE221}  XML Data Source Object 3.0
{F5078F3F-C551-11D3-89B9-0000F81FE221}  XML Moniker 3.0
{F5078F40-C551-11D3-89B9-0000F81FE221}  XML Document 3.0
{F5078F41-C551-11D3-89B9-0000F81FE221}  XML Island 3.0
{f507f854-308b-401e-a1b7-b55ba6ba679a}  Association Property Handler
{F515306D-0156-11d2-81EA-0000F87557DB}  Emboss
{F515306E-0156-11d2-81EA-0000F87557DB}  Engrave
{F5175861-2688-11d0-9C5E-00AA00A45957}  Subscription Folder
{F54309BB-0AFA-4BE0-B6D9-810F01F4DEE6}  Microsoft Support App Window Manager
{F556F9B2-C810-44A2-BA7A-3AB8C24E666D}  GenValObject Outer Class
{F55C5B4C-517D-11D1-AB57-00C04FD9159E}  Microsoft WBEM NT Eventlog Event Provider
{F562A2C8-E850-4F05-8E7A-E7192E4E6C23}  PSFactoryBuffer
{F5668FDF-340B-4BE2-8402-748EA156BB91}  CloudExperienceHost Synchronization
Implementation
{F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}  Security and Maintenance Shell Service
Object
{F582A54C-90D3-45b3-9860-EE3143AA85A0}  HomeGroup Named Property Store XML
{F595677C-076D-4E7F-AC39-4A644DC5DFD7}  User Assist
{f59aa553-8309-46ca-9736-1ac3c62d6031}  Device Display Status Manager
{F5A55D36-8750-432C-AB52-AD49A016EABC}  Microsoft WMI Provider Subsystem Binding
Factory
{f5a8b627-4d46-4d65-92f3-73626ae31971}  Explorer command store
{F5B63656-069D-4E80-B4FD-9E0DB16604D8}
{f5d121ed-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.User
{f5d121ee-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Group
{f5d121ef-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Domain
{f5d121f0-c8ac-11d0-bcdb-00c04fd8d5b6}  DsPropertyPages.Contact
```

Page 118

SOFTWARE OUTPUT.txt

```
{f5d121f3-c8ac-11d0-bcdb-00c04fd8d5b6}   DsPropertyPages.Volume
{f5d121f4-c8ac-11d0-bcdb-00c04fd8d5b6}   DsPropertyPages.Computer
{F5D3E63B-CB0F-4628-A478-6D8244BE36B1}
{F5F75737-2843-4F22-933D-C76A97CDA62F}   Microsoft WMI Provider Subsystem Decoupled
Basic Event Provider
{F5FB2C77-0E2F-4A16-A381-3E560C68BC83}   Removable Drives
{f60163ce-2b8d-458d-ab2c-40f215767514}   CLSID_IndexScopeFiller
{F60C3E02-214A-462b-9B07-56EA38545A13}   Move-To Menu
{F6166DAD-D3BE-4ebd-8419-9B5EAD8D0EC7}   ShellItemArray Shell Namespace helper
{F618C514-DFB8-11D1-A2CF-00805FC79235}   Catalog2 Class
{F61FFEC1-754F-11d0-80CA-00AA005B4383}   BandProxy
{F62D062C-4732-44D2-BD62-124B8AE1657C}   WMPlayer PluginsPropPage Class
{f65817c8-dd85-4136-89f0-b9d12939f2c4}   IsolatedMessageDialogFactory
{f6b13ba7-d626-45e5-82c5-26e596114dc0}   WFP Clients Extensible Helper Class
{F6B6E965-E9B2-444B-9286-10C9152EDBC5}   History Vault
{F6B96EDA-1A94-4476-A85F-4D3DC7B39C3F}   DvbSiParser Class
{F6BEC032-233E-4B58-BEE9-DE13942BF136}   PSFactoryBuffer
{f6c29334-47dc-4397-9150-f549cf1d4861}   BufferProxy
{F6C3AC3E-E642-4795-A9F2-9B3AB94EAC5D}   Cached File Updater Merge Handler Helpers
{F6D90F11-9C73-11D3-B32E-00C04F990BB4}   XML DOM Document
{F6D90F12-9C73-11D3-B32E-00C04F990BB4}   Free Threaded XML DOM Document
{F6D90F14-9C73-11D3-B32E-00C04F990BB4}   XML Data Source Object
{F6D90F16-9C73-11D3-B32E-00C04F990BB4}   XML HTTP
{F6EFEABD-3370-4AA0-A4FD-88BADC3B1A39}   SpeechServiceWinRTApi.ProxyStubFactory
{F6F05056-37FA-4DAF-8A51-40A8F14E0F62}   Sync Provider Object Cache
{f7300245-1f4b-41ba-8948-6fd392064494}   Show Hidden Files Explorer Command
{F73C1438-71B4-4D91-AD13-1F889A03AC67}   PSFactoryBuffer
{f744e496-1b5a-489e-81dc-fbd7ac6298a8}   Microsoft PenInputPanel Control
{F74B1266-FF39-4B62-8B6B-29C09920852C}   PSFactoryBuffer
{F751293B-DC01-468D-925C-2B3619582720}
CLSID_SoftLandingNotificationActivationCallback
{F753E28A-00AA-4537-A4C4-CAA197D44DD0}   PSFactoryBuffer
{F778C6B4-C08B-11D2-976C-00C04F79DB19}
{F77C0A7D-7395-45c5-BDFC-B096BF6C4DA0}   Bluewire Paired Devices Menu
{f792beee-aeaf-4ebb-ab14-8bc5c8c695a8}   Media Foundation MP2demux
{F79A6BF9-7415-4CF3-AE10-4559509ABC3C}   Sound Event Scheme Handler
{F7A4F1DA-96C3-4BCF-BEB3-1D9FFDE89EE9}   ComCacheCleanup 1.0 Object
{F7AFD75B-BF8C-4a11-BDB9-04AD66182F84}   MF Video Presenter 2
{F7B9271E-46D8-4B6A-B5CF-E6A4F7F49732}   Alternates Class
{f7c0039a-4762-488a-b4b3-760ef9a1ba9b}   Provides access to a portable device using
IPortableDevice for multi-threaded applications (aggregates the free-threaded
marshaler)
{F7CDD0DF-887D-463F-AF57-0E442B5C233B}   Authentication UI CredUI Out of Proc
Helper for AppContainer Clients
{F7ECB841-7EB6-41EB-BAEA-E2145F7348C6}   Wired Network Pre-CFE Page
{F7F4A1B6-8E87-452f-A2D7-3077F508DBC0}   RandomDissolve
{f7fa3149-91e7-43b7-8040-b707688ced1a}   CloudExperienceHost Create System Object
Server
{F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
{F7FF39BA-FA79-11E4-87DA-8F461D5D46B0}   SpWASAudioBurstRead Class
{f7ffe0a0-a4f5-44b5-949e-15ed2bc66f9d}   MSScreen 9 encoder DMO
{f81b1b56-7613-4ee4-bc05-1fab5de5c07e}   MF MPEG-4 Property Handler
{f81e9010-6ea4-11ce-a7ff-00aa003ca9f6}   Shell extensions for sharing
{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}   Sync Registration
{F82DF8F7-8B9F-442E-A48C-818EA735FF9B}   Pen and Touch Control Panel
{F8383852-FCD3-11d1-A6B9-006097DF5BD4}   Progress Dialog
{F8388A40-D5BB-11D0-BE5A-0080C706568E}   Infinite Pin Tee Filter
{f83cbf45-1c37-4ca1-a78a-28bcb91642ec}   CD Audio Burning Hook
{F83DAC1C-9BB9-4f2b-B619-09819DA81B0E}   IE Registry Tree Options Utility
{F84431A3-A1BE-40FC-BAFA-84851B344AF8}   ReadingModeExtractedContent
{F8462F08-715D-4AA3-8A6E-3D3B5EC282D7}   CloudExperienceHost Synchronization
Default Implementation
{F857B5CD-68AD-4012-8527-AB3A8E56F620}   RADCApiWorkspace Class
```

Page 119

SOFTWARE OUTPUT.txt

| | |
|---|---|
| {f85d5d94-6851-44f7-bb3a-bfd0949abf1d} | Tree property value cache |
| {F86DEAA3-3A0C-4CF6-8E1F-747FED85AB4E} | Is Windows Genuine Command |
| {f86fa3ab-70d2-4fc7-9c99-fcbf05467f3a} | |
| {F87B28F1-DA9A-4F35-8EC0-800EFCF26B83} | SPPUIObjectInteractive Class |
| {f8842f8e-dafe-4b37-9d38-4e0714a61149} | CastServer |
| {F885120E-3789-4fd9-865E-DC9B4A6412D2} | IARPUninstallStringLauncher |
| {F8900A80-4885-4722-A655-7A60F7596E3A} | Update CSP |
| {F89E9E58-BD2F-4008-9AC2-0F816C09F4EE} | SoftKbdIMX Class |
| {F8A0B131-5F68-486c-8040-7E8FC3C85BB6} | WLIDCredentialProvider |
| {F8A254BD-D0D2-456d-B2C4-A6720B3E35F4} | CFileActivatedEventArgsProxy |
| {f8a56d3e-e304-4a9f-a916-5187019d7759} | |
| {f8a97f86-95af-416d-87aa-88d7c42e0e7c} | |
| PrintTaskConfigurationSaveRequestProxyServer | |
| {f8b8412b-dea3-4130-b36c-5e8be73106ac} | CLSID_PreviewHtml |
| {f8c2ab3b-17bc-41da-9758-339d7dbf2d88} | Previous Versions Results Folder |
| {F8D0708C-A86F-4CBA-A55A-F2081BD47721} | |
| {f8d1da80-9aea-4ca4-ba41-bee6fca037b1} | Show Library In Nav Pane verb |
| {F8E307FB-6D45-4AD3-9993-66CD5A529659} | MF Media Sharing Engine Class Factory |
| {F8FB6E07-55E6-4BB9-96BC-2393A039CEE7} | UIGlobalNotify Class |
| {F90B5F36-367B-402A-9DD1-BC0FD59D8F62} | |
| {F90FE5FE-E88B-4578-9C81-79210FD53D41} | Infrastructure Adapter Page Selection |
| Class | |
| {f91b9abc-985b-4c04-b5e7-9c7099fc2cda} | CADProvider |
| {F91D96C7-8509-4D0B-AB26-A0DD10904BB7} | CMpeg2Stream |
| {F935DC22-1CF0-11D0-ADB9-00C04FD58A0B} | Windows Script Host Shell Object |
| {F935DC26-1CF0-11D0-ADB9-00C04FD58A0B} | Windows Script Host Network Object |
| {F94CDF40-02D6-4E79-89F7-B5357F3B1A39} | Immersive Shell Hook Service |
| {F963C5CF-A659-4A93-9638-CAF3CD277D13} | DVD State |
| {F975AF2C-9A51-4AF0-91EA-06038698CE38} | DirectPlay8 Diagnostics Object |
| {F9769A06-7ACA-4E39-9CFB-97BB35F0E77E} | BDA Tuning Model Auxiliary Inputs Tuning |
| Space | |
| {F97B8A60-31AD-11CF-B2DE-00DD01101B85} | Stretch |
| {F9A7AB61-C0BC-490e-A7FE-BFF26B327A3F} | OpenSearch Result Context Menu |
| {F9A874B6-F8A8-4D73-B5A8-AB610816828B} | Terminal Services Connection Manager Class |
| {f9bcb2f0-7df0-4a39-932e-bdef29dfb16b} | Authentication UI Session Control |
| {F9BD3AE7-F595-47F0-B194-B6F40B8D9FFE} | ContinuousBackgroundTaskPolicy |
| {F9EBBF2D-0C5D-4BF1-AE24-A30F7796D178} | PSFactoryBuffer |
| {F9EFBEC2-4302-11D2-952A-00C04FA34F05} | Light |
| {FA10746C-9B63-4b6c-BC49-FC300EA5F256} | Enhanced Video Renderer |
| {FA2C37A7-2D1E-444F-AD7B-D946823A7072} | SpSharedRecoInst Class |
| {FA3E1D55-16DF-446d-872E-BD04D4F39C93} | CUserPropPages Class |
| {FA4B375A-45B4-4D45-8440-263957B11623} | Microsoft DVBS Network Provider |
| {FA5FE7C5-6A1D-4B11-B41F-F959D6C76500} | Microsoft MPEG-2 Media Foundation Media |
| Sink | |
| {fa61e9f8-580e-4575-ab01-4a62c31fcf43} | Initialize AutoPlay Foreground Control |
| {FA6D33D4-9405-4BA5-9983-12604AC8E77A} | Miracast Sink Scheme Handler |
| {FA735D10-205D-451B-9EE8-E171F2214EF0} | MSASR Locale Handler Class (2052) |
| {FA77A74E-E109-11D0-AD6E-00C04FD8FDFF} | WBEM Registry Event Provider |
| {FA7C375B-66A7-4280-879D-FD459C84BB02} | webDVD Adminitration class |
| {fa7cfdb5-80b3-44d6-b564-f71e6ebb465d} | Windows Push Notification Polling Url |
| Handler | |
| {FA869D29-BA80-4D7D-A867-0DF126F980A5} | MF ADTS Parser Class Factory |
| {FA8A68B2-C864-4BA2-AD53-D3876A87494B} | StreamBufferConfig |
| {FA9342F0-B15B-473C-A746-14FCD4C4A6AA} | |
| {fa996453-47cf-4e5a-8df6-67f93a046ebb} | Window Size Converter |
| {FAC1D9C0-0296-11D1-A840-00A0C92C9D5D} | DiskManagement.SnapInAbout |
| {FAC67227-E178-4fab-9FEA-B4E77D3DBE7D} | Video Extension Class |
| {FAD7C22E-971B-4681-B836-83FAB87D74C2} | LockScreenSettingsProvider |
| {FAE517E7-1B31-47B6-840B-14D7D910AD48} | User-pinned tile manager |
| {faeb54c4-f66f-4806-83a0-805299f5e3ad} | Microsoft Feeds Manager (scripting) |
| {FAF53CC4-BD73-4E36-83F1-2B23F46E513E} | VssEvent |
| {faf85f2e-a8e7-414d-a3e9-6b9e7b4a51ed} | |
| {FB012959-F4F6-44D7-9D09-DAA087A9DB57} | |

Page 120

SOFTWARE OUTPUT.txt

```
{FB11047A-4051-4d1d-9DCA-C80C5DF98D70}  CSimpleWAPNodeProcessor
{FB1E042E-6772-4834-B1BF-F03F120E5F36}  RASGCW Non UI Finish Class
{FB2FDC4F-7DD0-4ACE-9B1E-36E5C2F98D27}  Set Network Location Page Class
{FB40360C-547E-4956-A3B9-D4418859BA66}
{fb479c02-9ec4-4fed-8599-debe037452cb}  Shell Hardware Mixed Content Handler
Cancelled
{FB4D76FE-8863-4027-9D8A-4A00BEDF74D7}  SmStore
{fb647f50-2192-49e0-a68f-5775434058c7}  CMVEngine
{FB64825E-498C-45E8-ADD4-37E0C4FC68A6}  SBE Stats - Mpeg2 Video Stream Analysis
{FB67F8D9-03A1-42b5-979A-1577F0193611}  Record Source XML
{FB74F625-7D25-4455-B840-7B870B5B9322}  Windows Media SDK MSB Source Plugin
{FBDBD7C2-8E45-4468-A76C-8C832456E850}  NodeCache
{fbeb8a05-beee-4442-804e-409d6c4515e9}  ShellFolder for CD Burning
{fbebb71b-a592-4880-b096-9429ebe119db}  Extensible L2Sec Helper Class
{FC1EE10B-7EF6-41B5-BB60-98D26DD9FCD1}
{FC220AD8-A72A-4EE8-926E-0B7AD152A020}  MXXMLWriter
{FC31D09D-D059-4551-9A28-B88A4181EC29}  SpAudioFormat Class
{FC3CD69D-BD08-436F-A284-1641E2236DDA}  Windows.Networking.ProxyStubFactory
{FC46B571-5D16-4DCE-8F26-F7138C09C768}  Browser Setting Monitor
{FC47060E-6153-4B34-B975-8E4121EB7F3C}  DirectPlay8 Thread Pool Object
{fc470800-12e0-4da3-81f3-e67240d19093}  CLSID_WindowsStoreSilentInstaller
{FC48CC30-4F3E-4fa1-803B-AD0E196A83B1}  AccClientDocMgr Class
{FC5B8A24-DB05-4A01-8388-22EDF6C2BBBA}  Bidi Spooler APIs
{FC5EEAF6-2001-11DF-ADB9-F4CE462D9137}  Hotspot Auth Engine Singleton
{FC772AB0-0C7F-11D3-8FF2-00A0C9224CF4}  BDA MPEG2 Transport Information Filter
{FC80316A-0752-400d-AA2E-86DE4F6C26EF}  Record Sharing XML
{FC8E372E-8847-4E45-B724-F676B1CACC7D}  UPnP 1.0 Property Plugin
{FCC152B7-F372-11D0-8E00-00C04FD7C08B}  DVD Graph Builder
{fcc2867c-69ea-4d85-8058-7c214e611c97}  Authentication UI Terminal Services Bump
Dialog Server
{FCC74B77-EC3E-4dd8-A80B-008A702075A9}  ARP UninstallString Launcher
{fccf70c8-f4d7-4d8b-8c17-cd6715e37fff}  Search Control
{FCDC2CF5-ABCD-4BA5-94DA-1823AE06FE2B}  CorrelationEngine Class
{FCDECE00-A39D-11D0-ABE7-00AA0064D470}  ScriptoSys Class
{FCF7A6F2-3300-4386-9A4F-0DD4E3226507}  WmiPerf Instance Provider
{fcf8ebcb-d6cd-4f87-be38-d40b90ef2fb8}  Desktop Execute Open Verb
{FD0A5AF3-B41D-11D2-9C95-00C04F7971E0}  IBDA_DeviceControl
{FD209E2E-813B-41C0-8646-4C3E9C917511}  Microsoft WMI IPMI Provider
{FD215A13-A26A-44FF-BA3A-9109F278E28F}  MF Mux Sink Class Factory
{FD30033D-C508-491E-AE43-0075E46DED83}  UIManager
{FD351EA1-4173-4AF4-821D-80D4AE979048}  Stream Buffer V2 Source
{FD4F53E0-65DC-11D1-AB64-00C04FD9159E}  Microsoft WBEM NT Eventlog Instance
Provider
{FD688BBD-31ED-4DB7-A723-934927D38367}
{FD6F2917-326E-405B-8B10-DC93A013A73B}  Windows.Security.Cryptography
{FD78DA08-2964-40BF-AE00-72EA8155CB53}  MediaCoreVideoStabilizationEffect
{FD7F2B29-24D0-4B5C-B177-592C39F9CA10}  psfactorybuffer
{FD853CD9-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeInternational
{FD853CDB-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeBody
{FD853CDC-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessageParts
{FD853CDD-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeAllocator
{FD853CDE-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeSecurity
{FD853CDF-7F86-11d0-8252-00C04FD85AB4}  CLSID_IVirtualStream
{FD853CE0-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeHeaderTable
{FD853CE1-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimePropertySet
{FD853CE2-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessageTree
{FD853CE3-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimeMessage
{FD853CE6-7F86-11d0-8252-00C04FD85AB4}  CLSID_ISMTPTransport
{FD853CE7-7F86-11d0-8252-00C04FD85AB4}  CLSID_IPOP3Transport
{FD853CE8-7F86-11d0-8252-00C04FD85AB4}  CLSID_INNTPTransport
{FD853CE9-7F86-11d0-8252-00C04FD85AB4}  CLSID_IRASTransport
{FD853CEA-7F86-11d0-8252-00C04FD85AB4}  CLSID_IRangeList
{FD853CEB-7F86-11d0-8252-00C04FD85AB4}  CLSID_IIMAPTransport
```

Page 121

```
                    SOFTWARE  OUTPUT.txt
  {FD853CED-7F86-11d0-8252-00C04FD85AB4}  CLSID_IMimePropertySchema
  {fd8d3a5f-6066-11d1-8c13-00c04fd8d503}  Microsoft OrganizationUnit Extension
  {fd8d7f86-2f0c-43bb-b225-97ac3c04567b}  Generic Handle Marshaller
  {FDA74D11-C4A6-4577-9F73-D7CA8586E10C}  Proximity UX Host
  {FDA74D11-C4A6-4577-9F73-D7CA8586E10D}  MP UX Host
  {fdb00e52-a214-4aa1-8fba-4357bb0072ec}  Windows Antimalware Scan Interface
implementation
  {fdb3c379-7d69-4d39-b975-a621b00007be}  CImeSettingsCangjie
  {FDD384CC-78C6-4E6D-8694-1DACBEE57F96}  PSFactoryBuffer
  {FDDB1402-6A7D-4044-B85B-3AC449824BE8}  Application View Manager
  {FDE7673D-2E19-4145-8376-BBD58C4BC7BA}  IE Custom MRU AutoCompleted List
  {fe081f7f-67dc-4f4e-a74a-d6555cdc8efb}  Background activation of toast action
  {fe0bfe76-18b7-4ea4-a9ca-7277eef48747}  Cloud Experience Host Admin Elevation
Broker Manager
  {fe1290f0-cfbd-11cf-a330-00aa00c16e65}  @%SystemRoot%\system32\dsquery.dll,-553
  {FE12CD81-5158-4bd8-A37C-A621BC0E143B}
  {FE217CB2-0B2C-48c9-90CA-8D8BCA79248D}  Teredo Helper Class
  {FE3C02B0-B9FF-4A45-AE19-E9A8D4893511}  WebTokenRequest Object
  {fe5afcf2-e681-4ada-9703-ef39b8ecb9bf}  Library Description
  {FE62FDE5-E0D8-4118-9FA3-45D31A5AEA0F}  OOBE Account Error Page
  {FE6B11C3-C72E-4061-86C6-9D163121F229}  Microsoft Feeds Manager
  {FE6CBCD1-20A2-44F7-8A9C-BE3B161577A9}  CrossProcMessageEvent Class
  {FE7A7E7B-BB31-498C-9299-4F4DDC10B26F}
  {fe7c0d2b-27f1-4e97-951b-cf6e165eeab6}  TSMFActivate Class
  {fe841493-835c-4fa3-b6cc-b4b2d4719848}  EnumEnhancedStorageACT Class
  {FE883157-CEBD-4570-B7A2-E4FE06ABE626}  WSecEdit RSOP Security Settings Class
  {FE92BB18-77C1-451A-83E8-8420D74E4B1C}  FhSettingHandler Class
  {FE9AF5C0-D3B6-11CE-A5B6-00AA00680C3F}  WBEM Registry Instance Provider
  {FEA4300C-7959-4147-B26A-2377B9E7A91D}  DirectSoundFullDuplex Object
  {FEB50740-7BEF-11CE-9BD9-0000E202599C}  MPEG Video Codec
  {FEC52D45-D657-42c3-B43E-BF64B95E7072}  WIA Preview Component
  {fecd606e-7161-4cbc-a868-4703867823ea}  WMDM Transcode Property Page
  {FEEAAA2B-16F4-46F6-84BB-831197DD3D75}  TableManager Class
  {FEF10FA2-355E-4e06-9381-9B24D7F7CC88}
  {FF036D13-5D4B-46DD-B10F-106693D9FE4F}
  {FF151822-B0BF-11D1-A80D-000000000000}  Microsoft OLE DB Root Binder for Internet
Publishing
  {ff183a37-b6da-4d32-bb24-157b282ffa48}  CLSID_ApplicationSearchScopeFactory
  {FF2A742B-CA25-4507-BD93-6BA9B8E8965F}  Fat MSM Helper Class
  {FF2AB3A5-5EEA-4538-8F8F-C169CCD40200}  Windows.Devices.Radios.ProxyStubFactory
  {FF2F95A4-C6A1-4B48-BC87-8709250E0D03}  PSFactoryBuffer
  {FF302BD3-3DC6-4680-9384-621A7FF574F4}  CLSID_SearchSelectionService
  {ff363bfe-4941-4179-a81c-f3f1ca72d820}  HomeGroup SSO
  {FF393560-C2A7-11CF-BFF4-444553540000}  History
  {FF3AE31D-55B0-4945-BDE9-622ABB334C1A}  WABSyncConfigUI
  {ff48dba4-60ef-4201-aa87-54103eef594e}  UIAutomation Client Central Class
  {FF5265E8-6D8B-4BD4-A52D-8D99008E04C8}  PSFactoryBuffer
  {ff609cc7-d34d-4049-a1aa-2293517ffcc6}  SetBackgroundContextMenu
  {FF658520-21A7-4AE1-A72A-D5A2D937138C}  Microsoft XPS Shell Metadata Handler
  {ff8a32e3-a9a7-4093-b9c4-5b5b4f30ab63}  CLSID_ResultShape
  {ff8a71c2-7eb8-418b-950d-3b49f43f024f}  CWinCredProvider
  {ff9e6131-a8c1-4188-aa03-82e9f10a05a8}  Elevatable Shortcut
  {FFB8655F-81B9-4fce-B89C-9A6BA76D13E7}  Shell Execute Hardware Event Handler
  {FFCDB781-D71C-4D10-BD5F-0492EAFFD90A}  PSFactoryBuffer
  {FFCECE86-332F-49B4-B9EE-7FECEFAD3E10}  MCCS SyncStatusNotification
  {FFD0B1B9-0BC0-41F1-BF9B-A931E870A991}  CLSID_MIMEUUDecoder
  {ffd90217-f7c2-4434-9ee1-6f1b530db20f}  XML Feed Moniker
  {ffe1df5f-9f06-46d3-af27-f1fc10d63892}  HomeGroup CPL Advanced Settings Writer
  {FFE1E5FE-F1F0-48C8-953E-72BA272F2744}  EntAppSvc
  {FFE2A43C-56B9-4bf5-9A79-CC6D4285608A}  Windows Photo Viewer Image Verbs
  {FFE8C349-2BB1-411F-93CE-0364C5F9FD9F}  MTF Server
Fri Jul 10 09:07:55 2015 Z
  {0823B6F8-F499-4d5e-B885-EA9CB4F43B24}  Component Based Servicing Worker
```

Page 122

SOFTWARE OUTPUT.txt
```
Fri Jul 10 09:05:39 2015 Z
   {4729dc2b-36ff-405f-bd36-f45113adb052}   Component Based Servicing Retry Session
   {75207391-23F2-4396-85F0-8FDB879ED0ED}   Component Based Servicing Session
Proxy/Stub
   {752073A1-23F2-4396-85F0-8FDB879ED0ED}   Component Based Servicing Session
   {9F7D7BB5-20B3-11DA-81A5-0030F1642E3C}   SettingsEngine Class
----------------------------------------
cmd_shell v.20130405
(Software) Gets shell open cmds for various file types

Classes\exefile\shell\open\command
LastWrite Time Fri Jul 10 11:05:55 2015 (UTC)
   Cmd: "%1" %*

Classes\cmdfile\shell\open\command
LastWrite Time Fri Jul 10 11:05:55 2015 (UTC)
   Cmd: "%1" %*

Classes\batfile\shell\open\command
LastWrite Time Fri Jul 10 11:05:55 2015 (UTC)
   Cmd: "%1" %*

Classes\csfile\shell\open\command not found.

Classes\htafile\shell\open\command
LastWrite Time Fri Jul 10 13:19:47 2015 (UTC)
   Cmd: C:\Windows\SysWOW64\mshta.exe "%1"
{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}%U{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} %*

Classes\piffile\shell\open\command
LastWrite Time Fri Jul 10 11:05:56 2015 (UTC)
   Cmd: "%1" %*


Clients\StartMenuInternet\IExplore.exe\shell\open\command
LastWrite Time Fri Jul 10 13:19:49 2015 (UTC)
   Cmd: C:\Program Files\Internet Explorer\iexplore.exe
----------------------------------------
codeid v.20100608
(Software) Gets CodeIdentifier DefaultLevel value

CodeID
Policies\Microsoft\Windows\Safer\CodeIdentifiers
   LastWrite time: Fri Jul 10 12:20:50 2015 Z

----------------------------------------
ctrlpnl v.20100116
(Software) Get Control Panel info from Software hive


Microsoft\Windows\CurrentVersion\Control Panel

Cpls key has no values.
don't load key
appwiz.cpl
bthprops.cpl
desk.cpl
Firewall.cpl
hdwwiz.cpl
inetcpl.cpl
intl.cpl
irprops.cpl
joy.cpl
```

Page 123

SOFTWARE OUTPUT.txt

```
main.cpl
mmsys.cpl
ncpa.cpl
powercfg.cpl
sysdm.cpl
tabletpc.cpl
telephon.cpl
timedate.cpl
```

System.ControlPanel.Category [Fri Jul 10 11:05:46 2015 UTC]
Category -1,4
   %SystemRoot%\System32\Speech\SpeechUX\sapi.cpl

{305CA226-D286-468e-B848-2B2E8E697B74} 2 [Thu Aug 13 22:30:54 2015 UTC]
Sounds, Speech, and Audio Devices
   %SystemRoot%\System32\RTSnMg64.cpl


----------------------------------------
defbrowser v.20091116
(Software) Gets default browser setting from HKLM

Default Browser Check #1
Clients\StartMenuInternet
LastWrite Time Thu Jul 16 03:46:14 2015 (UTC)

Default Browser : IEXPLORE.EXE

Default Browser Check #2
Classes\HTTP\shell\open\command
LastWrite Time Wed Mar 23 09:52:53 2016 (UTC)

Default Browser = "C:\Program Files\Internet Explorer\iexplore.exe" %1
----------------------------------------
Launching direct v.20120513
Microsoft

Wow6432Node\Microsoft
Thu Apr 21 02:57:46 2016    DirectDraw\MostRecentApplication - Install.exe

----------------------------------------
disablesr v.20120914
(Software) Gets the value that turns System Restore either on or off

Microsoft\Windows NT\CurrentVersion\SystemRestore
LastWrite Time Sun Apr 17 19:55:17 2016 (UTC)

DisableSR value not found.
----------------------------------------
drivers32 v.20130408
(Software) Get values from the Drivers32 key

Microsoft\Windows NT\CurrentVersion\Drivers32
LastWrite Time Tue Mar 22 13:15:54 2016 (UTC)
   vidc.iyuv - iyuv_32.dll
   vidc.uyvy - msyuv.dll
   wave2 - wdmaud.drv
   wave3 - wdmaud.drv
   aux1 - wdmaud.drv
   aux - wdmaud.drv
   mixer3 - wdmaud.drv
   vidc.i420 - iyuv_32.dll
   msacm.imaadpcm - imaadp32.acm
```

Page 124

SOFTWARE OUTPUT.txt

```
    vidc.yvu9 - tsbyuv.dll
    MSVideo8 - VfWWDM32.dll
    midi - wdmaud.drv
    msacm.msadpcm - msadp32.acm
    wavemapper - msacm32.drv
    midimapper - midimap.dll
    vidc.yvyu - msyuv.dll
    vidc.msvc - msvidc32.dll
    mixer1 - wdmaud.drv
    midi3 - wdmaud.drv
    vidc.mrle - msrle32.dll
    mixer2 - wdmaud.drv
    mixer - wdmaud.drv
    vidc.yuy2 - msyuv.dll
    msacm.l3acm - C:\Windows\System32\l3codeca.acm
    midi2 - wdmaud.drv
    msacm.msgsm610 - msgsm32.acm
    wave - wdmaud.drv
    msacm.msg711 - msg711.acm
    wave1 - wdmaud.drv
    midi1 - wdmaud.drv

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
LastWrite Time Tue Mar 22 13:15:54 2016 (UTC)
    vidc.iyuv - iyuv_32.dll
    vidc.uyvy - msyuv.dll
    wave2 - wdmaud.drv
    wave3 - wdmaud.drv
    aux1 - wdmaud.drv
    aux - wdmaud.drv
    vidc.cvid - iccvid.dll
    mixer3 - wdmaud.drv
    vidc.i420 - iyuv_32.dll
    msacm.imaadpcm - imaadp32.acm
    vidc.yvu9 - tsbyuv.dll
    midi - wdmaud.drv
    msacm.msadpcm - msadp32.acm
    wavemapper - msacm32.drv
    midimapper - midimap.dll
    vidc.yvyu - msyuv.dll
    vidc.msvc - msvidc32.dll
    mixer1 - wdmaud.drv
    midi3 - wdmaud.drv
    vidc.mrle - msrle32.dll
    mixer2 - wdmaud.drv
    mixer - wdmaud.drv
    msacm.l3acm - C:\Windows\SysWOW64\l3codeca.acm
    vidc.yuy2 - msyuv.dll
    midi2 - wdmaud.drv
    msacm.msgsm610 - msgsm32.acm
    wave - wdmaud.drv
    msacm.msg711 - msg711.acm
    wave1 - wdmaud.drv
    midi1 - wdmaud.drv

-------------------------------------
drwatson v.20081219
(Software) Gets Dr. Watson settings from Software hive

Microsoft\Windows NT\CurrentVersion\AeDebug
LastWrite Time Fri Jul 10 11:05:46 2015 (UTC)
Debugging is Disabled
```

Page 125

SOFTWARE OUTPUT.txt

Microsoft\DrWatson not found.

Analysis Tips: For Dr. Watson settings information check:
http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/RegistryTips/Registry
Tools/DrWatson.html
-------------------------------------
emdmgmt v.20120207
(Software) Gets contents of EMDMgmt subkeys and values

EMDMgmt
Microsoft\Windows NT\CurrentVersion\EMDMgmt
LastWrite Time Fri Sep 11 09:46:21 2015 (UTC)

FWVQAAWJVQJJACer
    LastWrite: Thu Aug 13 23:28:21 2015 Z
    VSN: 402A-5C4D

FWVQGPIDYLVBRecovery
    LastWrite: Fri Sep 11 09:42:48 2015 Z
    VSN: 3C2C-C7D2

FWVQSJPQAHREACer
    LastWrite: Fri Sep 11 09:42:47 2015 Z
    VSN: 402A-5C4D

FWVQSPNVWSVHRecovery
    LastWrite: Thu Aug 13 23:28:22 2015 Z
    VSN: 3C2C-C7D2

Unknown&ESP
    LastWrite: Fri Sep 11 09:46:21 2015 Z
    VSN: 8027-5A8E

Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100
    LastWrite: Fri Sep 11 09:42:48 2015 Z
    SN: 05NEOR7OF6IS3C1M&0
    Vol Name: NOTEBOOK
    VSN: 1A02-2E77


-------------------------------------
ie_version v.20140717
(Software) Get IE version and build

Microsoft\Internet Explorer
LastWrite Time Sun Apr 17 00:44:02 2016 (UTC)

IE Build    = 910240
IE Version = 9.11.10240.16384
svcUpdateVersion (IE 10/11) = 11.0.30
svcVersion (IE 10/11)       = 11.0.10240.16766
-------------------------------------
imagefile v.20131007
(Software) Checks IFEO subkeys for Debugger & CWDIllegalInDllSearch values

Microsoft\Windows NT\CurrentVersion\Image File Execution Options
No Debugger/CWDIllegalInDllSearch values found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options not
found.
-------------------------------------
init_dlls v.20110309
(Software) Check for odd **pInit_Dlls keys

Page 126

SOFTWARE OUTPUT.txt

init_dlls
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite: Fri Jul 10 12:20:33 2015

LoadAppInit_DLLs
------------------------------------------
installedcomp v.20130911
(Software) Get info about Installed Components and StubPath values

Microsoft\Active Setup\Installed Components
LastWrite Time Thu Jul 16 03:40:55 2015 (UTC)

Sun Apr 17 00:44:02 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.10,0,10240,16766, U
Wed Mar 23 09:52:53 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,10240,0, C:\Windows\System32\ie4uinit.exe -UserConfig
Wed Mar 23 09:48:50 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Mar 23 09:48:50 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,10011,16506
Wed Mar 23 09:48:50 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe
/FirstLogon
Thu Jul 16 03:41:07 2015 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,
v.2,0,50727,0
Fri Jul 10 13:19:49 2015
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\System32\Rundll32.exe C:\Windows\System32\mscories.dll,Install
Fri Jul 10 11:06:04 2015 (UTC),{C49181C5-51A7-39B8-A058-B35C7BAD6E1F},.NETFramework,
v.4,0,30319,0
Fri Jul 10 11:05:13 2015 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, /UserInstall
Fri Jul 10 11:05:13 2015 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.10,0,10240,16384, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
Fri Jul 10 11:05:13 2015 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEX,
v.4,71,1113,0
Fri Jul 10 11:05:13 2015 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Fri Jul 10 11:05:13 2015 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Fri Jul 10 11:05:13 2015 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.10,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,10240,0
Fri Jul 10 11:05:13 2015 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.10,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0

Wow6432Node\Microsoft\Active Setup\Installed Components
LastWrite Time Tue Apr 12 20:56:27 2016 (UTC)

Sun Apr 17 00:44:02 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
Page 127

SOFTWARE OUTPUT.txt
v.10,0,10240,16766, U
Tue Apr 12 20:56:27 2016 (UTC),{E5D12C4E-7B4F-11D3-B5C9-0050045C3C96},Yahoo!
Messenger, v.0.0.0.0
Wed Mar 23 09:52:53 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,10240,0, C:\Windows\System32\ie4uinit.exe -UserConfig
Wed Mar 23 09:48:50 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Mar 23 09:48:50 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,10011,16506
Wed Mar 23 09:48:50 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe
/FirstLogon
Wed Mar 23 09:48:50 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Mar 23 09:48:50 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,10011,16506
Wed Mar 23 09:48:50 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,10011,16506, %SystemRoot%\system32\unregmp2.exe
/FirstLogon
Tue Mar 22 11:22:11 2016 (UTC),{981b174d-7733-4e7f-b89d-6545a7c21838},, C:\Program
Files (x86)\Amazon\Amazon1ButtonApp\Amazon1ButtonTaskbarApp.exe /pin:
Thu Jul 16 03:41:07 2015 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,
v.2,0,50727,0
Thu Jul 16 03:40:55 2015 (UTC),{7C028AF8-F614-47B3-82DA-BA94E41B1089},.NETFramework,
v.2,0,50727,0
Fri Jul 10 13:19:52 2015
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install
Fri Jul 10 13:19:49 2015
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,
C:\Windows\System32\Rundll32.exe C:\Windows\System32\mscories.dll,Install
Fri Jul 10 11:06:04 2015 (UTC),{C49181C5-51A7-39B8-A058-B35C7BAD6E1F},.NETFramework,
v.4,0,30319,0
Fri Jul 10 11:06:01 2015 (UTC),{D3D70DDE-B3B4-33DE-A8CD-808A85D68682},.NETFramework,
v.4,0,30319,0
Fri Jul 10 11:05:13 2015 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, /UserInstall
Fri Jul 10 11:05:13 2015 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.10,0,10240,16384, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
Fri Jul 10 11:05:13 2015 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEX,
v.4,71,1113,0
Fri Jul 10 11:05:13 2015 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Fri Jul 10 11:05:13 2015 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Fri Jul 10 11:05:13 2015 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.10,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,10240,0
Fri Jul 10 11:05:13 2015 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.10,0,10240,16384
Fri Jul 10 11:05:13 2015 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0

Page 128

SOFTWARE OUTPUT.txt
Fri Jul 10 11:05:09 2015 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,
v.10,0,10240,16384, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
Fri Jul 10 11:05:09 2015 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEX,
v.4,71,1113,0
Fri Jul 10 11:05:09 2015 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Fri Jul 10 11:05:09 2015 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Fri Jul 10 11:05:09 2015 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},
v.10,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},
Fri Jul 10 11:05:09 2015 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,10240,0
Fri Jul 10 11:05:09 2015 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.10,0,10240,16384
Fri Jul 10 11:05:09 2015 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0
----------------------------------------
Launching installer v.20120917
(Software) Determines product install information

Installer
Microsoft\Windows\CurrentVersion\Installer\UserData

User SID: S-1-5-18
Key      : 000021091A0090400000000000F01FEC
LastWrite: Tue Mar 22 13:32:11 2016
20160327 - Microsoft Office OneNote MUI (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 000021095110904000000000000F01FEC
LastWrite: Tue Mar 22 13:31:24 2016
20160327 - Microsoft Office Shared Setup Metadata MUI (English) 2007 12.0.6612.1000
(Microsoft Corporation)

Key      : 0000210961009040000000000000F01FEC
LastWrite: Tue Mar 22 13:31:48 2016
20160327 - Microsoft Office Excel MUI (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 000021096110904001000000000F01FEC
LastWrite: Tue Mar 22 13:33:05 2016
20160327 - Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007
12.0.6612.1000 (Microsoft Corporation)

Key      : 0000210981009040000000000000F01FEC
LastWrite: Tue Mar 22 13:32:33 2016
20160327 - Microsoft Office PowerPoint MUI (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002109A200000001000000000F01FEC
LastWrite: Tue Mar 22 10:34:58 2016
20160331 - Microsoft Office Office 64-bit Components 2007 12.0.6612.1000 (Microsoft
Page 129

SOFTWARE OUTPUT.txt
Corporation)

Key      : 00002109A20090400100000000F01FEC
LastWrite: Tue Mar 22 13:32:49 2016
20160327 - Microsoft Office Shared 64-bit MUI (English) 2007 12.0.6612.1000
(Microsoft Corporation)

Key      : 00002109B10090400000000000F01FEC
LastWrite: Tue Mar 22 10:34:45 2016
20160327 - Microsoft Office Word MUI (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002109C20090400000000000F01FEC
LastWrite: Tue Mar 22 10:34:35 2016
20160322 - Microsoft Office Proofing (English) 2007 12.0.4518.1014 (Microsoft
Corporation)

Key      : 00002109E60090400000000000F01FEC
LastWrite: Tue Mar 22 13:31:01 2016
20160331 - Microsoft Office Shared MUI (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002109F10090400000000000F01FEC
LastWrite: Tue Mar 22 10:34:26 2016
20160327 - Microsoft Office Proof (English) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002109F100A0C00000000000F01FEC
LastWrite: Tue Mar 22 10:33:31 2016
20160327 - Microsoft Office Proof (Spanish) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002109F100C0400000000000F01FEC
LastWrite: Tue Mar 22 10:33:57 2016
20160327 - Microsoft Office Proof (French) 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00002119F20000000000000000F01FEC
LastWrite: Tue Mar 22 10:37:22 2016
20160414 - Microsoft Office Home and Student 2007 12.0.6612.1000 (Microsoft
Corporation)

Key      : 00004109500200000000000000F01FEC
LastWrite: Sun Apr 10 21:38:43 2016
20160414 - Microsoft Office File Validation Add-In 14.0.5130.5003 (Microsoft
Corporation)

Key      : 05A2A6B343AC2104EBA2FD66FDE538EA
LastWrite: Thu Aug 13 22:15:02 2015
20150813 - Intel(R) Trusted Execution Engine 1.1.1.1 (Intel Corporation)

Key      : 1af2a8da7e60d0b429d7e6453b3d0182
LastWrite: Wed Mar 23 09:42:47 2016
20160323 - Microsoft Visual C++ 2005 Redistributable (x64) 8.0.61000 (Microsoft
Corporation)

Key      : 1BF4A48A307DBD84980E866B94D98210
LastWrite: Thu Aug 13 22:24:41 2015
20150813 - Qualcomm Atheros Bluetooth Suite (64) 10.0.1.0 (Qualcomm Atheros)

Key      : 27E8763E3E8719F49ABF198367FFD62A
LastWrite: Thu Aug 13 22:35:38 2015
20150813 - Acer Quick Access 2.00.3005 (Acer Incorporated)
Page 130

SOFTWARE OUTPUT.txt

```
Key      : 2F817A21753214D4E9F18185A374547F
LastWrite: Thu Jul 16 03:47:00 2015
20150715 - Acer UEIP Framework 2.01.3002 (Acer Incorporated)

Key      : 2F98DA5B3D306024487810288900D70D
LastWrite: Tue Mar 22 13:27:09 2016
20160322 - abPhoto 3.06.2000.22 (Acer Incorporated)

Key      : 411A73A4F20755044A6B6175D1A43535
LastWrite: Tue Mar 22 13:20:47 2016
20160322 - AOP Framework 3.13.2000.0 (Acer Incorporated)

Key      : 48E14FA18043A994C83988190F167291
LastWrite: Thu Jul 16 03:43:58 2015
20150715 - Care Center 2.00.3005 (Acer Incorporated)

Key      : 4EA42A62D9304AC4784BF2381208190F
LastWrite: Thu Apr 21 03:27:18 2016
20160420 - Java 8 Update 91 8.0.910.14 (Oracle Corporation)

Key      : 4ED25F19987B0B2439113A941FE04597
LastWrite: Thu Aug 13 22:37:25 2015
20150813 - Acer Power Management 7.00.8109 (Acer Incorporated)

Key      : 63AEB64B17B0E4A4EA1478426134AFA0
LastWrite: Thu Aug 13 22:39:04 2015
20150813 - PowerDVD 12.0 (CyberLink Corp.)

Key      : 67D6ECF5CD5FBA732B8B22BAC8DE1B4D
LastWrite: Fri Mar 25 12:28:54 2016
20160325 - Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
9.0.30729.6161 (Microsoft Corporation)

Key      : 6E815EB96CCE9A53884E7857C57002F0
LastWrite: Fri Mar 25 12:29:23 2016
20160325 - Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
9.0.30729.6161 (Microsoft Corporation)

Key      : 71B0DA5AD43FEB941A758C3B5DA2DC31
LastWrite: Tue Mar 22 13:30:40 2016
20160322 - Acer Portal 3.09.2002.0 (Acer Incorporated)

Key      : 72D5A39806E2C62498ABAE020245B5AF
LastWrite: Thu Aug 13 22:14:57 2015
20150813 - Intel(R) Trusted Execution Engine Driver 1.0.0.1064 (Intel Corporation)

Key      : 7AE62CD33E3035344942EE7B3AA45740
LastWrite: Tue Mar 22 13:15:31 2016
20160322 - eBay Worldwide 2.5.0427 (OEM)

Key      : 7C43C21609E58D74B9C5F017D78D7262
LastWrite: Wed Mar 23 10:30:27 2016
20160323 - swMSM 12.0.0.1 (Adobe Systems, Inc)

Key      : 8E7DA64665F2E024C82E4197C8BE2507
LastWrite: Thu Aug 13 22:17:26 2015
20150813 - Intel(R) Serial IO 99.16.55518 (Intel Corporation)

Key      : A38C15B2D5649AE4C9CDE19DE50DA96C
LastWrite: Thu Aug 13 22:15:47 2015
20150813 - DriverSetupUtility 1.00.3011 (Acer Incorporated)
```

Page 131

SOFTWARE OUTPUT.txt

```
Key      : C173E5AD3336A8D3394AF65D2BB0CCE6
LastWrite: Tue Mar 22 13:31:11 2016
20160325 - Microsoft Visual C++ 2010  x64 Redistributable - 10.0.30319 10.0.30319
(Microsoft Corporation)

Key      : c1c4f01781cc94c4c8fb1542c0981a2a
LastWrite: Tue Apr 12 20:55:49 2016
20160323 - Microsoft Visual C++ 2005 Redistributable 8.0.61001 (Microsoft
Corporation)

Key      : CFD2C1F142D260E3CB8B271543DA9F98
LastWrite: Thu Aug 13 22:38:15 2015
20150813 - Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
9.0.30729.4148 (Microsoft Corporation)

Key      : D04BB691875110D32B98EBCF771AA1E1
LastWrite: Tue Mar 22 13:27:17 2016
20160325 - Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319 10.0.30319
(Microsoft Corporation)

Key      : D20352A90C039D93DBF6126ECE614057
LastWrite: Thu Aug 13 22:24:07 2015
20150813 - Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 9.0.30729
(Microsoft Corporation)

Key      : DA0D586B8A2493A4B9EFC860F39AFA92
LastWrite: Thu Aug 13 22:16:14 2015
20150813 - Intel(R) Chipset Device Software 10.1.1.8 (Intel Corporation)

Key      : EFEE0228DC83E77358593193D847A0EC
LastWrite: Thu Aug 13 22:24:10 2015
20150813 - Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 9.0.30729
(Microsoft Corporation)

Key      : F5415905096AA504A9FB967C7A138943
LastWrite: Tue Mar 22 11:22:05 2016


Key      : F60730A4A66673047777F5728467D401
LastWrite: Thu Apr 21 03:27:57 2016
20160420 - Java Auto Updater 2.8.91.14 (Oracle Corporation)

Key      : FC24F0D439619D34DB8C9141D120E30E
LastWrite: Thu Aug 13 22:35:59 2015
20150813 - Explorer Agent 2.00.3001 (Acer Incorporated)

Key      : FDB3204A5D28D214D985C88291BEEFE2
LastWrite: Thu Aug 13 22:39:54 2015
20150813 - Foxit PhantomPDF 7.0.410.326 (Foxit Software Inc.)

----------------------------------------
kb950582 v.20081212
(Software) KB950582 - Gets autorun settings from HKLM hive

NoDriveTypeAutoRun value may not exist: Can't call method "get_data" on an undefined
value at C:\Users\mdickson\Desktop\Tools\rrv2.8/plugins\kb950582.pl line 71.

HonorAutorunSetting not found.

Autorun settings in the HKLM hive take precedence over those in
the HKCU hive.
----------------------------------------
LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not found.
```

Page 132

SOFTWARE OUTPUT.txt

Wow6432Node\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not
found.
LANDesk\Inventory\LogonHistory\Logons not found.
Wow6432Node\LANDesk\Inventory\LogonHistory\Logons not found.
-----------------------------------------
macaddr v.20090118
(Software)  --

Microsoft\Windows Genuine Advantage not found.
-----------------------------------------
mrt v.20080804
(Software) Check to see if Malicious Software Removal Tool has been run

Key Path: Microsoft\RemovalTools\MRT
LastWrite Time Fri Apr 15 03:27:31 2016 (UTC)

Version: 6F31010B-5919-41C2-94FB-E71E8EEE9C9A

Analysis Tip:  Go to http://support.microsoft.com/kb/891716/ to see when MRT
was last run.  According to the KB article, each time MRT is run, a new GUID
is written to the Version value.
-----------------------------------------
msis v.20090911
(Software) Determine MSI packages installed on the system


Classes\Installer\Products
LastWrite Time Thu Apr 21 03:28:17 2016 (UTC)

Thu Apr 21 03:27:57 2016 (UTC)
  Java Auto
Updater;C:\Users\DeputyGod\AppData\LocalLow\Oracle\Java\jre1.8.0_91\au.msi
Thu Apr 21 03:27:18 2016 (UTC)
  Java 8 Update
91;C:\Users\DeputyGod\AppData\LocalLow\Oracle\Java\jre1.8.0_91\jre1.8.0_91full.msi
Thu Apr 21 03:15:13 2016 (UTC)
  ;
  ;
  ;
  ;
Fri Apr 15 03:28:03 2016 (UTC)
  Microsoft Office Home and Student 2007;C:\MSOCache\All
Users\{91120000-002F-0000-0000-0000000FF1CE}-C\HomeStudentrWW.msi
Fri Apr 15 03:21:46 2016 (UTC)
  Microsoft Office File Validation Add-In;OFV.msi
Thu Mar 31 18:39:23 2016 (UTC)
  Microsoft Office Office 64-bit Components 2007;C:\MSOCache\All
Users\{91120000-002F-0000-0000-0000000FF1CE}-C\Office64WW.msi
Thu Mar 31 18:27:48 2016 (UTC)
  Microsoft Office Shared MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.msi
Sun Mar 27 12:35:57 2016 (UTC)
  Microsoft Office Proof (French) 2007;C:\MSOCache\All
Users\{90120000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.msi
Sun Mar 27 12:35:53 2016 (UTC)
  Microsoft Office Proof (Spanish) 2007;C:\MSOCache\All
Users\{90120000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.msi
Sun Mar 27 12:35:50 2016 (UTC)
  Microsoft Office Proof (English) 2007;C:\MSOCache\All
Users\{90120000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.msi
Sun Mar 27 12:32:51 2016 (UTC)
  Microsoft Office Word MUI (English) 2007;C:\MSOCache\All
Users\{90120000-001B-0409-0000-0000000FF1CE}-C\WordMUI.msi
Sun Mar 27 12:32:47 2016 (UTC)

Page 133

SOFTWARE OUTPUT.txt

Microsoft Office PowerPoint MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi
Sun Mar 27 12:32:41 2016 (UTC)
Microsoft Office OneNote MUI (English) 2007;C:\MSOCache\All
Users\{90120000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.msi
Sun Mar 27 12:32:30 2016 (UTC)
Microsoft Office Excel MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi
Sun Mar 27 12:32:22 2016 (UTC)
Microsoft Office Shared Setup Metadata MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.msi
Sun Mar 27 12:32:21 2016 (UTC)
Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.msi
Sun Mar 27 12:32:04 2016 (UTC)
Microsoft Office Shared 64-bit MUI (English) 2007;C:\MSOCache\All
Users\{90120000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.msi
Fri Mar 25 12:29:23 2016 (UTC)
Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.6161;c:\ae8a068287496a281cbf17538f1567\vc_red.msi
Fri Mar 25 12:28:54 2016 (UTC)
Microsoft Visual C++ 2008 Redistributable - x64
9.0.30729.6161;c:\26af00a2c8dedf09a27615fbffde78\vc_red.msi
Fri Mar 25 12:28:44 2016 (UTC)
Microsoft Visual C++ 2010  x86 Redistributable -
10.0.30319;c:\b8bde854d3048da3d3\vc_red.msi
Fri Mar 25 12:28:14 2016 (UTC)
Microsoft Visual C++ 2010  x64 Redistributable -
10.0.30319;c:\5e4f1385002db0294d4297f2eba4f7\vc_red.msi
Wed Mar 23 10:30:27 2016 (UTC)
swMSM;C:\Windows\SysWOW64\Adobe\Shockwave 12\swMSM.msi
Wed Mar 23 09:42:47 2016 (UTC)
Microsoft Visual C++ 2005 Redistributable
(x64);C:\Users\DEPUTY~1\AppData\Local\Temp\IXP000.TMP\vcredist.msi
Wed Mar 23 09:42:22 2016 (UTC)
Microsoft Visual C++ 2005
Redistributable;C:\Users\DEPUTY~1\AppData\Local\Temp\IXP000.TMP\vcredist.msi
Tue Mar 22 13:30:40 2016 (UTC)
Acer Portal;C:\Windows\TEMP\AcerPortal\AcerPortal.msi
Tue Mar 22 13:27:09 2016 (UTC)
abPhoto;C:\Windows\TEMP\clear.fi_photo_AOP\clear.fi_Photo.msi
Tue Mar 22 13:20:47 2016 (UTC)
AOP Framework;C:\Windows\TEMP\AOP\AOP.msi
Tue Mar 22 13:15:31 2016 (UTC)
eBay Worldwide;c:\oem\preload\app\ebayworldwide\Setup.msi
Tue Mar 22 10:34:35 2016 (UTC)
Microsoft Office Proofing (English) 2007;C:\MSOCache\All
Users\{90120000-002C-0409-0000-0000000FF1CE}-C\Proofing.msi
Thu Aug 13 22:39:54 2015 (UTC)
Foxit PhantomPDF;C:\ProgramData\Package
Cache\{A4023BDF-82D5-412D-9D58-8C2819EBFE2E}v7.0.410.326\Setup.msi
Thu Aug 13 22:39:21 2015 (UTC)
PowerDVD;C:\OEM\Preload\APP\PowerDVD\PowerDVD.msi
Thu Aug 13 22:38:15 2015 (UTC)
Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.4148;C:\1d98b1baa0706924d0b230dfa368\vc_red.msi
Thu Aug 13 22:37:25 2015 (UTC)
Acer Power Management;C:\OEM\Preload\Autorun\APP\Power
Management\Power_Management_x64.msi
Thu Aug 13 22:35:59 2015 (UTC)
Explorer Agent;c:\OEM\Preload\METRO\AcerExplorer2003006\Agent\AppAgent_x64.msi
Thu Aug 13 22:35:38 2015 (UTC)
Acer Quick Access;C:\OEM\Preload\APP\QuickAccess\QuickAccess_x64.msi
Page 134

SOFTWARE OUTPUT.txt
Thu Aug 13 22:24:41 2015 (UTC)

;C:\Users\Administrator\AppData\Local\Temp\{FB335D7A-8998-43AA-A717-D355F58691BD}\Qu
alcomm Atheros Bluetooth Suite (64).msi
Thu Aug 13 22:20:29 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x64
9.0.30729.17;c:\b80404e09512cfaf42\vc_red.msi
Thu Aug 13 22:20:03 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.17;c:\8ea5ba5383f3a722d77dbf4e0fd328\vc_red.msi
Thu Aug 13 22:17:26 2015 (UTC)
  Intel(R) Serial
IO;C:\Users\Administrator\AppData\Local\Temp\IIFD4F7.tmp\SerialIO_x64.msi
Thu Aug 13 22:16:14 2015 (UTC)
  Intel(R) Chipset Device Software;C:\ProgramData\Package
Cache\{B685D0AD-42A8-4A39-9BFE-8C063FA9AF29}v10.1.1.8\SetupChipsetx64.msi
Thu Aug 13 22:15:47 2015 (UTC)
  DriverSetupUtility;C:\OEM\Preload\Autorun\DRV\Intel NB_Chipset_M
Baytrail-M\AppAgent_x64.msi
Thu Aug 13 22:15:02 2015 (UTC)
  Intel(R) Trusted Execution
Engine;C:\Users\Administrator\AppData\Local\Temp\IIF7C8F.tmp\TXE_x64.msi
Thu Aug 13 22:14:57 2015 (UTC)
  Intel(R) Trusted Execution Engine
Driver;C:\Users\Administrator\AppData\Local\Temp\IIF7C8F.tmp\TXE_Driver_x64.msi
Thu Jul 16 03:47:00 2015 (UTC)
  Acer UEIP Framework;C:\OEM\Preload\Modules\UEIPFramework\UbtFrameworkInstaller.msi
Thu Jul 16 03:43:58 2015 (UTC)
  Care Center;C:\OEM\Preload\APP\AcerCareCenter\CareCenter_x64.msi
--------------------------------------
networkcards v.20080325
(Software) Get NetworkCards

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Qualcomm Atheros AR956x Wireless Network Adapter  [Fri Sep 11 09:41:39 2015]
Qualcomm Atheros AR956x Wireless Network Adapter  [Fri Sep 11 09:41:39 2015]
Realtek PCIe GBE Family Controller  [Fri Sep 11 09:41:39 2015]
--------------------------------------
Launching networklist v.20141204
(Software) Collects network info from Vista+ NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Braddock
   Key LastWrite    : Thu Apr 21 03:19:17 2016 UTC
   DateLastConnected: Wed Apr 20 23:19:17 2016
   DateCreated      : Tue Mar 22 09:06:02 2016
   DefaultGatewayMac: E0-3F-49-9A-7B-40
   Type             : wireless
   Category         : Private

--------------------------------------
networkuid v.20100312
(Software) Gets Network key UID value

Microsoft\Windows NT\CurrentVersion\Network not found.
--------------------------------------
product v.20100325
(Software) Get installed product info


Microsoft\Windows\CurrentVersion\Installer\UserData
Page 135

SOFTWARE OUTPUT.txt

S-1-5-18
Thu Apr 21 03:27:57 2016 Z
   Java Auto Updater v.2.8.91.14, 20160420
Thu Apr 21 03:27:18 2016 Z
   Java 8 Update 91 v.8.0.910.14, 20160420
Fri Apr 15 03:28:02 2016 Z
   Microsoft Office Home and Student 2007 v.12.0.6612.1000, 20160414
Fri Apr 15 03:21:45 2016 Z
   Microsoft Office File Validation Add-In v.14.0.5130.5003, 20160414
Tue Apr 12 20:55:49 2016 Z
   Microsoft Visual C++ 2005 Redistributable v.8.0.61001, 20160323
Thu Mar 31 18:39:23 2016 Z
   Microsoft Office Office 64-bit Components 2007 v.12.0.6612.1000, 20160331
Thu Mar 31 18:27:48 2016 Z
   Microsoft Office Shared MUI (English) 2007 v.12.0.6612.1000, 20160331
Sun Mar 27 12:35:57 2016 Z
   Microsoft Office Proof (French) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:35:53 2016 Z
   Microsoft Office Proof (Spanish) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:35:50 2016 Z
   Microsoft Office Proof (English) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:32:51 2016 Z
   Microsoft Office Word MUI (English) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:32:47 2016 Z
   Microsoft Office PowerPoint MUI (English) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:32:41 2016 Z
   Microsoft Office OneNote MUI (English) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:32:30 2016 Z
   Microsoft Office Excel MUI (English) 2007 v.12.0.6612.1000, 20160327
Sun Mar 27 12:32:22 2016 Z
   Microsoft Office Shared Setup Metadata MUI (English) 2007 v.12.0.6612.1000,
20160327
Sun Mar 27 12:32:21 2016 Z
   Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007 v.12.0.6612.1000,
20160327
Sun Mar 27 12:32:04 2016 Z
   Microsoft Office Shared 64-bit MUI (English) 2007 v.12.0.6612.1000, 20160327
Fri Mar 25 12:29:23 2016 Z
   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 v.9.0.30729.6161,
20160325
Fri Mar 25 12:28:54 2016 Z
   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161,
20160325
Fri Mar 25 12:28:44 2016 Z
   Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319 v.10.0.30319, 20160325
Fri Mar 25 12:28:14 2016 Z
   Microsoft Visual C++ 2010  x64 Redistributable - 10.0.30319 v.10.0.30319, 20160325
Wed Mar 23 10:30:27 2016 Z
   swMSM v.12.0.0.1, 20160323
Wed Mar 23 09:42:47 2016 Z
   Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000, 20160323
Tue Mar 22 13:30:40 2016 Z
   Acer Portal v.3.09.2002.0, 20160322
Tue Mar 22 13:27:09 2016 Z
   abPhoto v.3.06.2000.22, 20160322
Tue Mar 22 13:20:47 2016 Z
   AOP Framework v.3.13.2000.0, 20160322
Tue Mar 22 13:15:31 2016 Z
   eBay Worldwide v.2.5.0427, 20160322
Tue Mar 22 10:34:35 2016 Z
   Microsoft Office Proofing (English) 2007 v.12.0.4518.1014, 20160322
Thu Aug 13 22:39:54 2015 Z

Page 136

SOFTWARE OUTPUT.txt
```
  Foxit PhantomPDF v.7.0.410.326, 20150813
Thu Aug 13 22:39:04 2015 Z
  PowerDVD v.12.0, 20150813
Thu Aug 13 22:38:15 2015 Z
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148,
20150813
Thu Aug 13 22:37:25 2015 Z
  Acer Power Management v.7.00.8109, 20150813
Thu Aug 13 22:35:59 2015 Z
  Explorer Agent v.2.00.3001, 20150813
Thu Aug 13 22:35:38 2015 Z
  Acer Quick Access v.2.00.3005, 20150813
Thu Aug 13 22:24:41 2015 Z
  Qualcomm Atheros Bluetooth Suite (64) v.10.0.1.0, 20150813
Thu Aug 13 22:24:10 2015 Z
  Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 v.9.0.30729, 20150813
Thu Aug 13 22:24:07 2015 Z
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 v.9.0.30729, 20150813
Thu Aug 13 22:17:26 2015 Z
  Intel(R) Serial IO v.99.16.55518, 20150813
Thu Aug 13 22:16:14 2015 Z
  Intel(R) Chipset Device Software v.10.1.1.8, 20150813
Thu Aug 13 22:15:47 2015 Z
  DriverSetupUtility v.1.00.3011, 20150813
Thu Aug 13 22:15:02 2015 Z
  Intel(R) Trusted Execution Engine v.1.1.1.1, 20150813
Thu Aug 13 22:14:57 2015 Z
  Intel(R) Trusted Execution Engine Driver v.1.0.0.1064, 20150813
Thu Jul 16 03:47:00 2015 Z
  Acer UEIP Framework v.2.01.3002, 20150715
Thu Jul 16 03:43:58 2015 Z
  Care Center v.2.00.3005, 20150715
Thu Jan  1 00:00:00 1970 Z
  v.,


-----------------------------------------
profilelist v.20100219
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList
LastWrite Time Fri Mar 25 10:51:56 2016 (UTC)

Path       : %systemroot%\system32\config\systemprofile
SID        : S-1-5-18
LastWrite : Fri Jul 10 11:05:46 2015 (UTC)

Path       : C:\Windows\ServiceProfiles\LocalService
SID        : S-1-5-19
LastWrite : Fri Jul 10 12:20:42 2015 (UTC)

Path       : C:\Windows\ServiceProfiles\NetworkService
SID        : S-1-5-20
LastWrite : Fri Jul 10 12:20:42 2015 (UTC)

Path       : C:\Users\DeputyGod
SID        : S-1-5-21-670634337-3447264720-4152838973-1001
LastWrite : Thu Apr 21 04:41:01 2016 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)

Path       : C:\Users\Mallik
SID        : S-1-5-21-670634337-3447264720-4152838973-1002
LastWrite : Fri Mar 25 11:27:02 2016 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)
```
Page 137

SOFTWARE OUTPUT.txt

Domain Accounts
--------------------------------------------
regback v.20100219
(Software) List all tasks along with logfile name and last written date/time

regidle
Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Registry\RegIdleBackup
LastWrite: Fri Jul 10 11:06:00 2015

SD          ᴶ▥    ··      ¶  �7  |     ↑ ÿ  7    |    7   ¶ ÿ     |↕      ¶
  ↕        |ᴶ    ( © ↕  –    |P  ∧ó☼±d®ᴶ±L¢)¶±L!¦vv  ¶ © ↕        |‼    7    |
7   7   |      7
Id            {1DEDCFF4-858F-489C-8EB5-0985DB41E194}
Index     3
Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
LastWrite Time Thu Apr 21 03:11:28 2016 (UTC)

Path          : \Microsoft\Windows\WS\License Validation
Dynamicinfo   : {00CC4A28-27D2-4A45-8876-CCBEE8CC0B6A}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path          : \Microsoft\Windows\ApplicationData\DsSvcCleanup
Dynamicinfo   : {00EEBA9C-F9EF-4272-B793-C830FBADD359}
LastWrite : Tue Apr 19 18:25:36 2016 (UTC)

Path          : \Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck
Dynamicinfo   : {02070E6A-19C9-464D-BB59-1F5110BAFF81}
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path          : \Microsoft\Windows\Shell\IndexerAutomaticMaintenance
Dynamicinfo   : {0220876D-72FC-48B2-9F66-864A70DA9864}
LastWrite : Tue Apr 19 18:25:36 2016 (UTC)

Path          : \Microsoft\Windows\Plug and Play\Device Install Group Policy
Dynamicinfo   : {038C5AA2-771C-42F6-BC6B-C7E1A01B25DA}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path          : \Quick Access
Dynamicinfo   : {08BC4179-63C2-4C6B-8100-DA7220B3655D}
LastWrite : Thu Apr 21 03:20:34 2016 (UTC)

Path          : \Microsoft\Windows\Task Manager\Interactive
Dynamicinfo   : {090BCDC9-7907-4164-96AA-746FAB30F521}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path          : \User_Feed_Synchronization-{6A1A9780-C921-411E-B5C8-5DC3652CB49E}
Dynamicinfo   : {0A704B2D-2C77-4123-AB20-D0ADD9A80B10}
LastWrite : Thu Apr 21 02:49:12 2016 (UTC)

Path          : \Microsoft\Windows\Diagnosis\Scheduled
Dynamicinfo   : {0B00D51A-5243-4AB8-BDE0-0C129880402E}
LastWrite : Fri Apr  1 16:31:15 2016 (UTC)

Path          : \Microsoft\Windows\Workplace Join\Automatic-Device-Join
Dynamicinfo   : {0CCA7916-2916-4F12-BD32-1E3BE31E1269}
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path          : \Microsoft\Windows\CloudExperienceHost\CreateObjectTask
Dynamicinfo   : {100B8472-CF48-4837-9BAA-CA1710FD66D4}
LastWrite : Tue Mar 22 13:13:00 2016 (UTC)

Page 138

SOFTWARE OUTPUT.txt

```
Path          : \Microsoft\Windows\Plug and Play\Device Install Reboot Required
Dynamicinfo   : {12CBA7A2-4B9A-4943-B1AE-35C2EE86BDB3}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path          : \Microsoft\Windows\Bluetooth\UninstallDeviceTask
Dynamicinfo   : {14C9EF7F-12E9-4B7B-8658-FF7B087A5B57}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path          : \Microsoft\Windows\UpdateOrchestrator\Schedule Scan
Dynamicinfo   : {1641F54C-1E57-4902-AB65-EE2B65E5629D}
LastWrite : Thu Apr 21 03:22:07 2016 (UTC)

Path          : \Microsoft\Windows\SettingSync\BackgroundUploadTask
Dynamicinfo   : {18E3AD12-4E0A-4293-AE32-2B1F14BF8C9C}
LastWrite : Fri Apr  1 16:30:05 2016 (UTC)

Path          : \Microsoft\Windows\WindowsUpdate\sihboot
Dynamicinfo   : {19865544-CE08-40BE-8B8C-87C47681433D}
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path          : \Microsoft\Windows\Location\Notifications
Dynamicinfo   : {1D3D099E-EE1E-4907-8BA2-BA8F12D11AA6}
LastWrite : Thu Apr 21 03:36:12 2016 (UTC)

Path          : \Microsoft\Windows\Registry\RegIdleBackup
Dynamicinfo   : {1DEDCFF4-858F-489C-8EB5-0985DB41E194}
LastWrite : Fri Apr 15 03:16:58 2016 (UTC)

Path          : \Microsoft\Windows\NetTrace\GatherNetworkInfo
Dynamicinfo   : {220E09D3-717B-4AC1-A52C-E49AC73C6276}
LastWrite : Fri Jul 10 12:21:43 2015 (UTC)

Path          : \FUBTrackingByPLD
Dynamicinfo   : {24819168-8C0C-405E-ABCE-29D95924D5B3}
LastWrite : Thu Apr 21 04:21:19 2016 (UTC)

Path          : \Microsoft\Windows\AppID\PolicyConverter
Dynamicinfo   : {25223772-CE6D-40BA-86D2-A9402FDC452F}
LastWrite : Fri Jul 10 12:21:43 2015 (UTC)

Path          : \Microsoft\Windows\SystemRestore\SR
Dynamicinfo   : {2BC0E7B3-5593-45D7-A657-9173E23D7988}
LastWrite : Sun Apr 17 19:55:17 2016 (UTC)

Path          : \Microsoft\Windows\SpacePort\SpaceAgentTask
Dynamicinfo   : {2BC9287F-22E5-4FCD-A005-5E2EA29C2E8E}
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path          : \Microsoft\Windows\Multimedia\SystemSoundsService
Dynamicinfo   : {2C62F5D5-5BA6-4CD4-9B68-83333E7542D6}
LastWrite : Thu Apr 21 04:41:01 2016 (UTC)

Path          : \Microsoft\Windows\CertificateServicesClient\KeyPreGenTask
Dynamicinfo   : {2C97A00A-1C5C-4318-B5CC-8A1A126B77F9}
LastWrite : Thu Jul 16 04:10:05 2015 (UTC)

Path          : \Microsoft\Windows\WS\WSTask
Dynamicinfo   : {2D523C15-5732-476B-8033-59A6C253BF94}
LastWrite : Fri Jul 10 12:21:43 2015 (UTC)

Path          : \Microsoft\Windows\Customer Experience Improvement
Program\KernelCeipTask
Dynamicinfo   : {31509320-2872-4CF2-948C-A5AF2AA4A5F7}
```

Page 139

SOFTWARE OUTPUT.txt

Path        : \Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
DynamicInfo : {33C85A4E-A97E-447A-A6B7-C7E723SEFDA3}
LastWrite   : Tue Apr 19 01:29:35 2016 (UTC)

Path        : \Microsoft\Windows\Plug and Play\Sysprep Generalize Drivers
DynamicInfo : {347D4A14-684E-44F1-9137-D48C1C0DD5F4}
LastWrite   : Thu Jul 16 04:12:20 2015 (UTC)

Path        : \Microsoft\Windows\Shell\FamilySafetyRefresh
DynamicInfo : {3BBE2501-5D2B-4690-BE72-FEBAD0807ODA}
LastWrite   : Fri Jul 10 12:21:43 2015 (UTC)

Path        : \Avast Secureline
DynamicInfo : {3DF849C2-CC87-41F6-80F2-EAE16DBF4250}
LastWrite   : Thu Apr 21 04:41:00 2016 (UTC)

Path        : \Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
DynamicInfo : {3F6E048D-6404-433B-8F5F-CFF4D89BF89E}
LastWrite   : Wed Apr 20 07:14:49 2016 (UTC)

Path        : \Microsoft\Windows\wininet\CacheTask
DynamicInfo : {3F803BEA-B3F2-4D29-BC92-5840A270FFBF}
LastWrite   : Thu Apr 21 04:41:01 2016 (UTC)

Path        : \Microsoft\Windows\Feedback\Siuf\DmClient
DynamicInfo : {41160EA0-2088-4C3E-B4DB-805BBABC6B93}
LastWrite   : Tue Apr 19 18:25:37 2016 (UTC)

Path        : \McAfeeLogon
DynamicInfo : {4308A1C1-4714-4266-805D-0D4D72BD24D8}
LastWrite   : Thu Apr 21 04:40:56 2016 (UTC)

Path        : \Microsoft\Windows\Customer Experience Improvement Program\Consolidator
DynamicInfo : {43CFBA73-D7C3-48B7-B58C-1CE0DCB31AC1}
LastWrite   : Thu Apr 21 04:00:01 2016 (UTC)

Path        : \Microsoft\Windows\Maps\MapsUpdateTask
DynamicInfo : {4454A8D0-2E4E-4A02-BF67-48DF6A7BFAB4}
LastWrite   : Fri Jul 10 12:21:43 2015 (UTC)

Path        : \Microsoft\Windows\MUI\LPRemove
DynamicInfo : {4B94510D-E729-41CF-A9EE-6F56A2637F2A}
LastWrite   : Tue Apr 19 01:36:30 2016 (UTC)

Path        : \Microsoft\Windows\Work Folders\Work Folders Maintenance Work
DynamicInfo : {4C3E72CC-C30C-48C7-8F2E-4B79F2AD9413}
LastWrite   : Fri Apr 1 16:30:05 2016 (UTC)

Path        : \Microsoft\Windows\Time Synchronization\SynchronizeTime
DynamicInfo : {4D4ED500-8F48-4DD6-8029-429FAFD68C34}
LastWrite   : Sun Apr 17 19:45:13 2016 (UTC)

Path        : \Power Management
DynamicInfo : {4F0751B0-E510-4975-9C30-AFBA18BF8CEC}
LastWrite   : Thu Apr 21 03:20:34 2016 (UTC)

Path        : \Microsoft\Windows\Ras\MobilityManager
DynamicInfo : {51AC5DCB-2238-42E6-915A-3CE06195599AE}
LastWrite   : Fri Jul 10 12:21:43 2015 (UTC)

Page 140

SOFTWARE OUTPUT.txt

```
Path              : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319
Critical
Dynamicinfo       : {528E1DC6-B4B3-4AF7-BB3E-D31FEE182A94}
LastWrite : Sun Apr 17 19:55:14 2016 (UTC)

Path              : \Microsoft\Windows\TextServicesFramework\MsCtfMonitor
Dynamicinfo       : {57C9690E-01CA-43EF-929C-3531B21AD0C3}
LastWrite : Thu Apr 21 04:41:01 2016 (UTC)

Path              : \BacKGroundAgent
Dynamicinfo       : {5A1828CA-CE45-49AF-AB7B-0EBB4836727A}
LastWrite : Thu Apr 21 04:40:57 2016 (UTC)

Path              : \Microsoft\Windows\SettingSync\NetworkStateChangeTask
Dynamicinfo       : {5A910370-7644-4D87-B4FB-6BB3081D8C14}
LastWrite : Thu Apr 21 03:29:48 2016 (UTC)

Path              : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319
Dynamicinfo       : {5A9238A3-C9D6-4C86-8F26-15C15575D23D}
LastWrite : Tue Apr 19 18:25:50 2016 (UTC)

Path              : \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic
Dynamicinfo       : {5BB3ECA7-92D5-48DF-8FB7-52EB2ECEBD03}
LastWrite : Fri Apr  1 21:56:52 2016 (UTC)

Path              : \Microsoft\Windows\Sysmain\ResPriStaticDbSync
Dynamicinfo       : {5E5515C1-7D87-4904-B9CE-FD29EB2ADB72}
LastWrite : Tue Apr 19 01:36:29 2016 (UTC)

Path              : \Microsoft\Windows\UpdateOrchestrator\Policy Install
Dynamicinfo       : {611C823C-437B-46E7-9683-5312DFFCFD7B}
LastWrite : Fri Jul 10 12:22:45 2015 (UTC)

Path              : \Microsoft\Windows\Application Experience\StartupAppTask
Dynamicinfo       : {61CD214B-BF88-4D91-923A-1C0F93D740DD}
LastWrite : Fri Apr  1 16:30:03 2016 (UTC)

Path              : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319
64 Critical
Dynamicinfo       : {6371C53B-18F0-421F-B4A3-A5D105EA940F}
LastWrite : Sun Apr 17 19:52:29 2016 (UTC)

Path              : \Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask
Dynamicinfo       : {667C8231-5036-4830-892B-D675837E506E}
LastWrite : Fri Jul 10 12:21:43 2015 (UTC)

Path              : \Microsoft\Windows\Sysmain\HybridDriveCachePrepopulate
Dynamicinfo       : {6829DA89-8DAC-468A-9436-8654BF975CF8}
LastWrite : Fri Jul 10 12:21:43 2015 (UTC)

Path              : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319
64
Dynamicinfo       : {6944CA49-98BB-47A3-A058-E4018B43D2E8}
LastWrite : Tue Apr 19 18:25:45 2016 (UTC)

Path              : \Microsoft\Windows\RecoveryEnvironment\VerifyWinRE
Dynamicinfo       : {6CA95ECB-D6F7-47BA-BD42-4AF1914D6E55}
LastWrite : Tue Mar 22 12:36:21 2016 (UTC)

Path              : \Microsoft\Windows\CertificateServicesClient\AikCertEnrollTask
Dynamicinfo       : {711EE2F9-A611-4773-AF8E-D4B278A6718D}
LastWrite : Thu Jul 16 03:35:49 2015 (UTC)
```

Page 141

SOFTWARE OUTPUT.txt

```
Path          : \Microsoft\Windows\Maps\MapsToastTask
Dynamicinfo   : {73551810-E5F4-433E-9494-0D00B55C855E}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path          : \Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser
Dynamicinfo   : {73D1EEFD-024B-4782-B722-EC764CE153E6}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path          : \Microsoft\Windows\UpdateOrchestrator\Resume On Boot
Dynamicinfo   : {744C9FEA-08B7-43E1-A729-0F94647D655C}
LastWrite : Thu Mar 24 10:52:38 2016 (UTC)

Path          : \Microsoft\Windows\WOF\WIM-Hash-Management
Dynamicinfo   : {78A1AA00-FD44-434C-8108-2C40D1578E4A}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path          : \Microsoft\Windows\Application Experience\ProgramDataUpdater
Dynamicinfo   : {78B77FA3-9D97-441D-97B6-68CEA40B4F74}
LastWrite : Tue Apr 19 18:26:53 2016 (UTC)

Path          : \Microsoft\Windows\UpdateOrchestrator\Reboot
Dynamicinfo   : {7A003965-A297-4DC6-B15B-852D798391E0}
LastWrite : Thu Apr 21 04:21:27 2016 (UTC)

Path          : \Microsoft\Windows\Time Synchronization\ForceSynchronizeTime
Dynamicinfo   : {7B0BDAEA-0EEC-4ED7-AE73-4D9D106322B3}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path          : \App Explorer
Dynamicinfo   : {7BEB14D9-CB1A-432D-A10B-B8DFBAA6C253}
LastWrite : Thu Apr 21 04:41:00 2016 (UTC)

Path          : \Microsoft\Windows\DiskCleanup\SilentCleanup
Dynamicinfo   : {80BD0F94-AC1F-45B7-B3AD-25E173E15F08}
LastWrite : Fri Apr  1 21:56:52 2016 (UTC)

Path          : \McAfee\McAfee Auto Maintenance Task Agent
Dynamicinfo   : {80DFFC9A-4F20-4B7F-8B8C-FAA3CE906FF9}
LastWrite : Thu Apr 21 03:11:18 2016 (UTC)

Path          : \Microsoft\Windows\Sysmain\HybridDriveCacheRebalance
Dynamicinfo   : {83226677-0E64-464F-A434-64538B4ABE1D}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path          : \Microsoft\Windows\UpdateOrchestrator\USO_UxBroker_ReadyToReboot
Dynamicinfo   : {848DCC36-520C-4946-BF68-C7EFFEFA2F84}
LastWrite : Fri Jul 10 12:22:45 2015 (UTC)

Path          : \avast! SL Update
Dynamicinfo   : {873DC160-5E70-4A92-BC94-9FB6BFAFF9A4}
LastWrite : Thu Apr 21 03:44:41 2016 (UTC)

Path          : \ACC
Dynamicinfo   : {8831D1F8-E6D0-4D0B-BCDA-19BAF52A02EB}
LastWrite : Thu Apr 21 04:34:36 2016 (UTC)

Path          : \ACCBackgroundApplication
Dynamicinfo   : {8CA7B7B3-3F6A-46B2-BD1A-9AFDDF32DD12}
LastWrite : Thu Apr 21 04:41:00 2016 (UTC)

Path          : \Microsoft\Windows\Clip\License Validation
Dynamicinfo   : {8DF84CB3-D8E0-4307-A35B-CA74E21786DB}
```

Page 142

SOFTWARE OUTPUT.txt
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path           : \Microsoft\Windows\CertificateServicesClient\SystemTask
Dynamicinfo    : {94526B46-C115-452D-9CA6-1497CA548E85}
LastWrite : Thu Apr 21 03:19:24 2016 (UTC)

Path           : \Microsoft\Windows\Windows Filtering
Platform\BfeOnServiceStartTypeChange
Dynamicinfo    : {95F3E121-B80B-4183-98C9-6A4B594C4161}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path           : \AcerCloud
Dynamicinfo    : {96446A1B-8545-4206-B0DD-6ABB1A8FA5D6}
LastWrite : Thu Apr 21 04:40:56 2016 (UTC)

Path           : \Microsoft\Windows\CertificateServicesClient\UserTask-Roam
Dynamicinfo    : {98CF5A2D-5D85-4188-86DA-E0B03A27E135}
LastWrite : Tue Apr 19 00:27:49 2016 (UTC)

Path           : \Microsoft\Windows\Active Directory Rights Management Services
Client\AD RMS Rights Policy Template Management (Automated)
Dynamicinfo    : {99B96646-1069-4CA3-B4F1-BE8D079CAE8A}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path           : \Microsoft\Windows\Device Setup\Metadata Refresh
Dynamicinfo    : {9BAB8F5A-4D45-4104-9895-8F05D88C195F}
LastWrite : Fri Apr  1 16:30:05 2016 (UTC)

Path           : \Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup
Dynamicinfo    : {9E25773C-3B56-402D-92A1-C1271B83F26C}
LastWrite : Tue Mar 22 13:28:02 2016 (UTC)

Path           : \Microsoft\Windows\UPnP\UPnPHostConfig
Dynamicinfo    : {A20B2CAE-96B0-4388-B8C9-A8AC43E1FEAA}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path           : \Microsoft\Windows\Windows Media Sharing\UpdateLibrary
Dynamicinfo    : {A29E9F64-8D95-4786-A7FB-1729E264ED80}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path           : \Software Update Application
Dynamicinfo    : {A2A04E3F-DD2B-4C05-B257-EA113A3E6DE4}
LastWrite : Thu Apr 21 03:19:36 2016 (UTC)

Path           : \Microsoft\Windows\UpdateOrchestrator\Maintenance Install
Dynamicinfo    : {A364E297-00AD-490D-900E-22AC34598C71}
LastWrite : Fri Apr 15 03:16:28 2016 (UTC)

Path           : \Microsoft\Windows\AppID\EDP Policy Manager
Dynamicinfo    : {A5B6CD85-1B57-49B9-BA80-5D5D65F02826}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path           : \Microsoft\Windows\Windows Error Reporting\QueueReporting
Dynamicinfo    : {A7AD0FAF-F382-4841-AF0E-E59A8B29A2EA}
LastWrite : Thu Apr 21 04:02:14 2016 (UTC)

Path           : \Microsoft\Windows\WindowsUpdate\Automatic App Update
Dynamicinfo    : {AC29E64E-3271-47BA-B8F1-914523CF379B}
LastWrite : Thu Apr 21 03:24:34 2016 (UTC)

Path           : \Microsoft\Windows\Shell\CreateObjectTask
Dynamicinfo    : {AE81D147-93CD-4431-A337-557A69F3A02F}
LastWrite : Thu Apr 21 02:47:41 2016 (UTC)
Page 143

SOFTWARE OUTPUT.txt

```
Path              : \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
Dynamicinfo       : {B071E173-DB92-4CA1-BD26-A4F2883DB6C5}
LastWrite : Tue Apr 19 18:27:58 2016 (UTC)

Path              :
\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTaskNetwork
Dynamicinfo       : {B3D6E2BD-8411-4981-BE29-896EDA3CDBC5}
LastWrite : Tue Mar 22 13:10:07 2016 (UTC)

Path              : \Microsoft\Windows\WindowsUpdate\Scheduled Start
Dynamicinfo       : {B68B60D0-0DFC-4300-A74D-E2D0F1765003}
LastWrite : Thu Apr 21 04:32:30 2016 (UTC)

Path              : \McAfee\McAfee Idle Detection Task
Dynamicinfo       : {B8B12CC1-44F0-4598-AE03-02ACEB5C10DF}
LastWrite : Thu Apr 21 03:11:18 2016 (UTC)

Path              : \Microsoft\Windows\WCM\WiFiTask
Dynamicinfo       : {B9B36D41-C776-424E-9A13-5387E17A2CEB}
LastWrite : Thu Apr 21 03:50:29 2016 (UTC)

Path              : \Microsoft\Windows\TPM\Tpm-Maintenance
Dynamicinfo       : {BA4D5D99-0A32-4F18-8F5B-8C7BAC45185A}
LastWrite : Thu Apr 21 03:19:05 2016 (UTC)

Path              : \Microsoft\Windows\User Profile Service\HiveUploadTask
Dynamicinfo       : {BDF53E5B-197D-4031-A282-0AAD1E6A7253}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path              : \Microsoft\Windows\UpdateOrchestrator\MusUx_LogonUpdateResults
Dynamicinfo       : {BF937198-888E-4694-83A1-2A5D9149B19C}
LastWrite : Thu Apr 21 03:21:30 2016 (UTC)

Path              : \Microsoft\Windows\PI\Secure-Boot-Update
Dynamicinfo       : {C186E3D5-138A-4C74-B2AD-21D4BD45D079}
LastWrite : Tue Mar 22 13:09:16 2016 (UTC)

Path              : \Microsoft\Windows\LanguageComponentsInstaller\Installation
Dynamicinfo       : {C2162702-FFEB-48C0-AA5F-2DA3A8887D61}
LastWrite : Thu Apr 21 03:34:33 2016 (UTC)

Path              : \ACCAgent
Dynamicinfo       : {C2824150-7469-43A9-A0F6-8C8AF48E2A9F}
LastWrite : Fri Apr  1 22:04:36 2016 (UTC)

Path              : \Microsoft\Windows\AppID\SmartScreenSpecific
Dynamicinfo       : {C33F4607-C279-4257-9039-34FF9FE1F21A}
LastWrite : Fri Apr  1 16:30:57 2016 (UTC)

Path              : \Microsoft\Windows\TPM\Tpm-HASCertRetr
Dynamicinfo       : {C56AFFD3-06B8-4A16-AF7E-F7A6EB3FAE9E}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path              : \Microsoft\Windows\WindowsUpdate\sih
Dynamicinfo       : {C5EE2EA2-5312-4D1F-B9D0-41B18DF31B78}
LastWrite : Wed Apr 20 23:14:00 2016 (UTC)

Path              : \Microsoft\Windows\Location\WindowsActionDialog
Dynamicinfo       : {C7A236B2-12E1-46DC-9501-3B1B0209CC09}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path              : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan for
```

Page 144

SOFTWARE OUTPUT.txt

Crash Recovery
Dynamicinfo    : {C9BAC386-E4A0-4615-BBC6-2FCDA8A8B067}
LastWrite : Fri Jul 10 12:21:44 2015 (UTC)

Path           : \Microsoft\Windows\Time Zone\SynchronizeTimeZone
Dynamicinfo    : {C9CC7661-60C0-46D7-8372-8BAF05FB10E1}
LastWrite : Fri Apr 15 03:18:32 2016 (UTC)

Path           : \UbtFrameworkService
Dynamicinfo    : {CDED0FE7-B8C0-45E5-9548-B9CA73096181}
LastWrite : Thu Apr 21 03:24:34 2016 (UTC)

Path           : \Microsoft\Windows\Active Directory Rights Management Services
Client\AD RMS Rights Policy Template Management (Manual)
Dynamicinfo    : {CE16D7B5-68D5-4B9B-A03A-A3AFF86EF011}
LastWrite : Fri Jul 10 12:21:42 2015 (UTC)

Path           : \Microsoft\Windows\Maintenance\WinSAT
Dynamicinfo    : {D1010C45-4003-46F0-B17E-D3284B0A5AC0}
LastWrite : Fri Apr  1 18:13:55 2016 (UTC)

Path           : \Microsoft\Windows\LanguageComponentsInstaller\Uninstallation
Dynamicinfo    : {D2401052-A382-42DE-9C79-D1CF3563F654}
LastWrite : Tue Mar 22 12:36:23 2016 (UTC)

Path           : \Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTaskLogon
Dynamicinfo    : {D35A0DF8-5C64-4005-B3D8-ED893905B7D9}
LastWrite : Tue Mar 22 13:10:07 2016 (UTC)

Path           : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents
Dynamicinfo    : {D6278A78-3EF8-4B66-A586-772BBB271889}
LastWrite : Fri Apr  1 21:56:52 2016 (UTC)

Path           : \Microsoft\Windows\WDI\ResolutionHost
Dynamicinfo    : {D7672D4C-1EC7-495D-B10C-66BAC959A587}
LastWrite : Sat Apr  2 18:35:43 2016 (UTC)

Path           : \Microsoft\Windows\Sysmain\WsSwapAssessmentTask
Dynamicinfo    : {D81EB21D-B1BA-4674-BFF3-879CFD0F69C3}
LastWrite : Fri Mar 25 12:34:16 2016 (UTC)

Path           : \Microsoft\Windows\DiskFootprint\Diagnostics
Dynamicinfo    : {DAF2BAE3-1C5B-4CB5-9F62-0911C031A15A}
LastWrite : Fri Apr 15 03:19:49 2016 (UTC)

Path           : \Microsoft\Windows\PI\Sqm-Tasks
Dynamicinfo    : {DC2B5D0F-DC88-4125-8BCA-06951B4A3CD2}
LastWrite : Tue Mar 22 12:35:57 2016 (UTC)

Path           : \Microsoft\Windows\CertificateServicesClient\UserTask
Dynamicinfo    : {DD251CE6-2367-4D18-B7D3-EE256A348FBB}
LastWrite : Thu Apr 21 03:19:36 2016 (UTC)

Path           : \Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask
Dynamicinfo    : {E1BDBB46-E3ED-499A-A766-1F95E532941A}
LastWrite : Thu Apr 21 03:22:57 2016 (UTC)

Path           : \Microsoft\Windows\Chkdsk\ProactiveScan
Dynamicinfo    : {E5F066B8-7C08-4642-8BBB-690E77367F0A}
LastWrite : Tue Apr 19 18:25:36 2016 (UTC)

Path           : \Microsoft\Windows\NetCfg\BindingWorkItemQueueHandler
Dynamicinfo    : {E6010D43-6AE7-4B59-8E67-EC78FD8E8E96}
Page 145

SOFTWARE OUTPUT.txt
LastWrite : Thu Apr 21 03:19:02 2016 (UTC)

Path         : \Microsoft\Windows\Shell\FamilySafetyMonitor
Dynamicinfo  : {E86A569D-2CCA-4FED-985B-074D08DCF577}
LastWrite : Fri Jul 10 12:21:45 2015 (UTC)

Path         : \Microsoft\Windows\Plug and Play\Plug and Play Cleanup
Dynamicinfo  : {E98AFDFB-4B5D-4DC1-9DCF-5DD16ED4B901}
LastWrite : Tue Mar 22 12:36:46 2016 (UTC)

Path         : \Microsoft\Windows\UpdateOrchestrator\USO_UxBroker_Display
Dynamicinfo  : {EA3F661E-B31C-44A9-B40C-E3D5D56149D4}
LastWrite : Thu Apr 21 04:21:25 2016 (UTC)

Path         : \Microsoft\Windows\Servicing\StartComponentCleanup
Dynamicinfo  : {EC62EDFD-2591-4129-BDE1-1E67C435DA01}
LastWrite : Fri Apr 15 03:21:13 2016 (UTC)

Path         : \Microsoft\Windows\WindowsColorSystem\Calibration Loader
Dynamicinfo  : {ECAAF1AF-8A34-4622-BD11-A0E5E98DF909}
LastWrite : Fri Jul 10 12:22:04 2015 (UTC)

Path         : \Microsoft\Windows\WOF\WIM-Hash-Validation
Dynamicinfo  : {EDA3F189-CEFF-44DF-B920-52E54F4FBA32}
LastWrite : Tue Mar 22 12:36:02 2016 (UTC)

Path         : \Microsoft\Windows\Autochk\Proxy
Dynamicinfo  : {EFC31D5C-DE7F-423F-806D-BDFDBF5871EC}
LastWrite : Sun Apr 17 19:45:24 2016 (UTC)

Path         : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan
Dynamicinfo  : {F1E8AA11-C616-43B1-834C-CB7F3F673380}
LastWrite : Fri Jul 10 12:21:39 2015 (UTC)

Path         : \Microsoft\Windows\Defrag\ScheduledDefrag
Dynamicinfo  : {F242C763-ACAC-4EF5-AF5C-82E9FA534691}
LastWrite : Fri Apr 15 03:29:13 2016 (UTC)

Path         : \Microsoft\Windows\FileHistory\File History (maintenance mode)
Dynamicinfo  : {F5CADC85-B320-4FC3-8498-06FB10F65D21}
LastWrite : Tue Apr 19 01:29:35 2016 (UTC)

Path         : \Microsoft\Windows\UpdateOrchestrator\MusUx_UpdateInterval
Dynamicinfo  : {F5D0AA44-EC17-42EE-9FC4-392CA9FF1DC9}
LastWrite : Tue Apr 12 00:37:24 2016 (UTC)

Path         :
\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
Dynamicinfo  : {F86B4620-9014-466B-A7DE-9EC3D73535BE}
LastWrite : Thu Jul 16 03:32:30 2015 (UTC)

Path         :
\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
Dynamicinfo  : {F92FFA8C-C649-4F28-8208-5F7C30AC788F}
LastWrite : Fri Apr 15 03:16:27 2016 (UTC)

Path         : \Microsoft\Windows\ApplicationData\CleanupTemporaryState
Dynamicinfo  : {FD678A25-1836-43B7-9291-92E25D88BF4A}
LastWrite : Tue Apr 19 18:25:36 2016 (UTC)

Path         : \Microsoft\Windows\Work Folders\Work Folders Logon Synchronization
Dynamicinfo  : {FFA27407-AC05-4A5A-B18A-EA230E27EB7A}
LastWrite : Thu Apr 21 03:24:34 2016 (UTC)
Page 146

SOFTWARE OUTPUT.txt

```
-------------------------------------------
removdev v.200800611
(Software) Parses Windows Portable Devices key (Vista)

RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Fri Sep 11 09:42:30 2015 (UTC)

Device     : DISK&VEN_JETFLASH&PROD_TRANSCEND_64GB&REV_1100
LastWrite  : Fri Sep 11 09:42:30 2015 (UTC)
SN         : 05NEOR7OF6IS3C1M&0
Drive      : NOTEBOOK

Device     : DISK&VEN_JETFLASH&PROD_TRANSCEND_64GB&REV_1100
LastWrite  : Fri Aug 14 02:01:21 2015 (UTC)
SN         : 124BWY3VPN6FOX4C&0
Drive      : WINPE TOOL

-------------------------------------------
renocide v.20130425
(Software) Check for Renocide malware

Microsoft\DRM\amty not found.
-------------------------------------------
schedagent v.20100817
(Software) Get SchedulingAgent key contents

Microsoft\SchedulingAgent
LastWrite Time Fri Jul 10 12:21:38 2015 (UTC)

OldName      = DESKTOP-M7P1NB6
TasksFolder  = %SystemRoot%\Tasks
-------------------------------------------
secctr v.20100310
(Software) Get data from Security Center key

secctr


Microsoft\Security Center
LastWrite Time Thu Apr 21 04:41:15 2016 (UTC)

cval                         0x00
-------------------------------------------
sfc v.20100305
(Software) Get SFC values

sfc v.20100305

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Apr 21 04:41:14 2016 (UTC)


Policies\Microsoft\Windows NT\Windows File Protection
LastWrite Time Fri Jul 10 11:05:50 2015 (UTC)

-------------------------------------------
shellexec v.20130410
(Software) Gets ShellExecuteHooks from Software hive

Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
LastWrite Time Fri Jul 10 11:05:46 2015 (UTC)
```
Page 147

SOFTWARE OUTPUT.txt

Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks has no values.  No
ShellExecuteHooks installed.
Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
LastWrite Time Fri Jul 10 11:05:46 2015 (UTC)

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks has no
values.  No ShellExecuteHooks installed.
-----------------------------------
shellext v.20100515
(Software) Gets Shell Extensions from Software hive

Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
LastWrite Time Thu Apr 21 03:15:17 2016 (UTC)

{F5175861-2688-11d0-9C5E-00AA00A45957}  Subscription Folder
   DLL: C:\Windows\System32\webcheck.dll
   Timestamp: Fri Jul 10 11:05:02 2015 Z

{60254CA5-953B-11CF-8C96-00AA00B8708C}  Shell extensions for Windows Script Host
   DLL: C:\Windows\System32\wshext.dll
   Timestamp: Fri Jul 10 11:05:04 2015 Z

{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}  Microsoft Office Metadata Handler
   DLL: C:\PROGRA~1\COMMON~1\MICROS~1\OFFICE12\msoshext.dll
   Timestamp: Tue Mar 22 10:34:57 2016 Z

{4F58F63F-244B-4c07-B29F-210BE59BE9B4}  .group shell extension handler
   DLL: %CommonProgramFiles%\System\wab32.dll
   Timestamp: Fri Jul 10 11:05:04 2015 Z

{289AF617-1CC3-42A6-926C-E6A863F0E3BA}  DLNA Namespace Extension
   DLL: C:\Windows\System32\dlnashext.dll
   Timestamp: Fri Jul 10 13:19:47 2015 Z

{08165EA0-E946-11CF-9C87-00AA005127ED}  WebCheckWebCrawler
   DLL: C:\Windows\System32\webcheck.dll
   Timestamp: Fri Jul 10 11:05:05 2015 Z

{C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97}  Microsoft Office Thumbnail Handler
   DLL: C:\PROGRA~1\COMMON~1\MICROS~1\OFFICE12\msoshext.dll
   Timestamp: Tue Mar 22 10:34:57 2016 Z

{7D559C10-9FE9-11d0-93F7-00AA0059CE02}  Code Download Agent
   DLL: C:\Windows\System32\webcheck.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{CF67796C-F57F-45F8-92FB-AD698826C602}  contact_wab_auto_file
   DLL: %CommonProgramFiles%\System\wab32.dll
   Timestamp: Fri Jul 10 11:05:02 2015 Z

{16C2C29D-0E5F-45f3-A445-03E03F587B7D}  group_wab_auto_file
   DLL: %CommonProgramFiles%\System\wab32.dll
   Timestamp: Fri Jul 10 11:05:04 2015 Z

{8082C5E6-4C27-48ec-A809-B8E1122E8F97}  .contact shell extension handler
   DLL: %CommonProgramFiles%\System\wab32.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{BFD468D2-D0A0-4bdc-878C-E69C2F5B435D}  Microsoft Windows Mail Html Preview Handler
   DLL: C:\Windows\System32\inetcomm.dll
   Timestamp: Fri Jul 10 11:05:02 2015 Z

Page 148

```
                              SOFTWARE OUTPUT.txt
{E6FB5E20-DE35-11CF-9C87-00AA005127ED}  WebCheck
   DLL:
   Timestamp: Thu Jan  1 00:00:00 1970 Z

{92dbad9f-5025-49b0-9078-2d78f935e341}  Microsoft Windows Mail Html Preview Handler
   DLL: C:\Windows\System32\inetcomm.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{0066D4B3-8DE0-4D08-AA83-EDD50E2431F0}  ELAN Control Panel
   DLL: %ProgramFiles%\Elantech\ETDMcpl.dll
   Timestamp: Thu Aug 13 22:28:13 2015 Z

{3DBEE9A1-C471-4B95-BBCA-F39310064458}  Microsoft Camera Raw Property Store
   DLL: C:\Windows\System32\WindowsCodecsRaw.dll
   Timestamp: Fri Jul 10 11:05:04 2015 Z

{b9815375-5d7f-4ce2-9245-c9d4da436930}  Microsoft Windows Mail Html Preview Handler
   DLL: C:\Windows\System32\inetcomm.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{f8b8412b-dea3-4130-b36c-5e8be73106ac}  Microsoft Windows Mail Html Preview Handler
   DLL: C:\Windows\System32\inetcomm.dll
   Timestamp: Fri Jul 10 11:05:02 2015 Z

{13D3C4B8-B179-4ebb-BF62-F704173E7448}  Windows Contact Preview Handler
   DLL: %CommonProgramFiles%\System\wab32.dll
   Timestamp: Fri Jul 10 11:05:04 2015 Z

{42042206-2D85-11D3-8CFF-005004838597}  Microsoft Office HTML Icon Handler
   DLL: C:\PROGRA~1\MICROS~1\Office12\MSOHEVI.DLL
   Timestamp: Tue Mar 22 10:34:57 2016 Z

{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB}  WebCheck SyncMgr Handler
   DLL: C:\Windows\System32\webcheck.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE}  Subscription Mgr
   DLL: C:\Windows\System32\webcheck.dll
   Timestamp: Fri Jul 10 11:05:03 2015 Z

{AF6FB31C-95D0-4A0E-8AFE-099969D8B689}  McAfee Vaults
   DLL: "C:\Program Files\McAfee\MAT\McPvNs.dll"
   Timestamp: Thu Apr 21 03:15:17 2016 Z

{0F8604A5-4ECE-4DE1-BA7D-CF10F8AA4F48}  Contacts folder
   DLL:
   Timestamp: Thu Jan  1 00:00:00 1970 Z

-------------------------------------------
shelloverlay v.20100308
(Software) Gets ShellIconOverlayIdentifiers values

shelloverlay
Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
LastWrite Time Tue Mar 22 13:31:12 2016 (UTC)

Tue Mar 22 13:31:12 2016 Z
    ACloudSynced  {5CCE71FA-9F61-4F24-9CD1-98D819B40D68}
    ACloudSyncing  {C1E1456F-C2D8-4C96-870D-35F1E13941EE}
    ACloudToBeSynced  {307523FA-DDC0-4068-983F-2A6B34627744}

Fri Jul 10 11:05:11 2015 Z
    OneDrive1  {BBACC218-34EA-4666-9D7A-C78F2274A524}
```

                              Page 149

```
                          SOFTWARE OUTPUT.txt
   OneDrive2   {5AB7172C-9C11-405C-8DD5-AF20F3606282}
   OneDrive3   {A78ED123-AB77-406B-9962-2A5D9D2F7F30}
   OneDrive4   {F241C880-6982-4CE5-8CF7-7085BA96DA5A}
   OneDrive5   {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E}
   EnhancedStorageShell   {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}
```

------------------------------------------
snapshot v.20080725
(Software) Check ActiveX comp kill bit; Access Snapshot

ActiveX Snapshot Vuln
Microsoft\Internet Explorer

IE Version = 9.11.10240.16384

GUID: {F0E42D50-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400

GUID: {F0E42D60-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400

GUID: {F2175210-368C-11D0-AD81-00A0C90DC8D9}
Compatibility Flags  0x400

------------------------------------------
soft_run v.20130603
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Thu Aug 13 23:02:01 2015 (UTC)
  RTHDVCPL - "C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s

Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Fri Apr  1 18:13:54 2016 (UTC)
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Thu Apr 21 03:27:57 2016 (UTC)
  SunJavaUpdateSched - "C:\Program Files (x86)\Common Files\Java\Java
Update\jusched.exe"
  ControlCenter4 - C:\Program Files (x86)\ControlCenter4\BrCcBoot.exe /autorun
  Malwarebytes Anti-Exploit - C:\Program Files (x86)\Malwarebytes
Anti-Exploit\mbae.exe
  abDocsDllLoader - C:\Program Files (x86)\Acer\abDocs\abDocsDllLoader.exe
  BrStsMon00 - C:\Program Files (x86)\Browny02\Brother\BrStMonW.exe /AUTORUN

Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Tue Apr 12 20:55:49 2016 (UTC)
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal
                          Page 150
```

SOFTWARE OUTPUT.txt
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

----------------------------------------
spp_clients v.20130429
(Software) Determines volumes monitored by VSS

SPP_Clients
Microsoft\Windows NT\CurrentVersion\SPP\Clients
LastWrite Time Thu Aug 13 22:14:51 2015 (UTC)

Monitored volumes: \\?\Volume{7fbc862e-e25b-407d-be01-f55b1d82ee42}\:Acer (C%3A)
----------------------------------------
sql_lastconnect v.20090112
(Software) MDAC cache of successful connections

Microsoft\MSSQLServer\Client\SuperSocketNetLib\LastConnect not found.
----------------------------------------
ssid v.20100301
(Software) Get WZCSVC SSID Info

Microsoft\WZCSVC\Parameters\Interfaces not found.
Microsoft\EAPOL\Parameters\Interfaces not found.
----------------------------------------
startmenuinternetapps_lm v.20101219
(SOFTWARE) Start Menu Internet Applications info

Start Menu Internet Applications


 [Fri Jul 10 11:05:53 2015 (UTC)] Contacts
 VALUE: (default) -> Address Book
 SUBKEY:   [Fri Jul 10 11:05:53 2015 (UTC)] Address Book


 [Tue Mar 22 10:37:06 2016 (UTC)] EnvelopeHost
 VALUE: no values.
 SUBKEY:   [Tue Mar 22 10:37:04 2016 (UTC)] Microsoft Excel
 SUBKEY:   [Tue Mar 22 10:37:06 2016 (UTC)] Microsoft Word


 [Tue Apr 12 20:56:21 2016 (UTC)] Internet Call
 VALUE: no values.
 SUBKEY:   [Tue Apr 12 20:56:21 2016 (UTC)] Yahoo! Messenger


 [Fri Jul 10 11:05:53 2015 (UTC)] Mail
 VALUE: no values.
 SUBKEY:   [Fri Jul 10 11:05:53 2015 (UTC)] Hotmail
 SUBKEY:   [Fri Jul 10 11:05:53 2015 (UTC)] Windows Mail


 [Fri Jul 10 11:05:53 2015 (UTC)] Media
 VALUE: no values.
 SUBKEY:   [Fri Jul 10 11:05:53 2015 (UTC)] Windows Media Player


 [Thu Jul 16 03:46:14 2015 (UTC)] StartMenuInternet
 VALUE: (default) -> IEXPLORE.EXE
 SUBKEY:   [Thu Aug 13 21:54:52 2015 (UTC)] FIREFOX.EXE
 SUBKEY:   [Fri Jul 10 13:19:49 2015 (UTC)] IEXPLORE.EXE

Page 151

SOFTWARE OUTPUT.txt
---------------------------------------------
svchost v.20100322
(Software) Get entries from SvcHost key

svchost


Microsoft\Windows NT\CurrentVersion\SvcHost
LastWrite Time Wed Mar 23 09:48:50 2016 (UTC)

bthaudiosvc        BthHFSrv
DcomLaunch
Power,LSM,BrokerInfrastructure,PlugPlay,DcomLaunch,SystemEventsBroker,DeviceInstall
defragsvc          defragsvc
LocalServiceAndNoImpersonation
TimeBroker,SSDPSRV,upnphost,SCardSvr,BthHFSrv,QWAVE,fdrespub,wcncsvc,SensrSvc
RPCSS              RpcEptMapper,RpcSs
sdrsvc             sdrsvc
utcsvc             DiagTrack
WepHostSvcGroup WepHostSvc
LocalService
nsi,WdiServiceHost,w32time,EventSystem,RemoteRegistry,WinHttpAutoProxySvc,SstpSvc,ne
tprofm,lltdsvc,FontCache,fdphost,bthserv,workfolderssvc,WebClient,CDPSvc,AJRouter,Li
censeManager
LocalSystemNetworkRestricted
WdiSystemHost,ScDeviceEnum,WiaRpc,trkwks,AudioEndpointBuilder,WUDFSvc,hidserv,dot3sv
c,DsSvc,WPDBusEnum,fhsvc,sysmain,NcbService,homegrouplistener,DeviceAssociationServi
ce,PcaSvc,Netman,TabletInputService,svsvc,SmsRouter,DevQueryBroker,wlansvc,EmbeddedM
ode,irmon,vmickvpexchange,vmicshutdown,vmicvss,vmicguestinterface,vmicvmsession,Stor
Svc,SensorService,UmRdpService
netsvcs
CertPropSvc,SCPolicySvc,lanmanserver,gpsvc,IKEEXT,iphlpsvc,seclogon,AppInfo,msiscsi,
EapHost,schedule,winmgmt,browser,ProfSvc,SessionEnv,wercplsupport,dosvc,wlidsvc,DcpS
vc,NcaSvc,NetSetupSvc,FastUserSwitchingCompatibility,Ias,Irmon,Nla,Ntmssvc,NWCWorkst
ation,Nwsapagent,Rasauto,Rasman,Remoteaccess,SENS,Sharedaccess,SRService,Tapisrv,Wmi
,WmdmPmSp,wuauserv,BITS,ShellHWDetection,LogonHours,PCAudit,helpsvc,uploadmgr,dmwapp
ushservice,XblGameSave,XboxNetApiSvc,UsoSvc,UserManager,lfsvc,DmEnrollmentSvc,XblAut
hManager,RetailDemo,BDESVC,DsmSvc,Themes
WerSvcGroup        wersvc
WbioSvcGroup       WbioSrvc
LocalServiceNoNetwork DPS,PLA,BFE,NcdAutoSetup,CoreMessagingRegistrar,mpssvc,WwanSvc
imgsvc             StiSvc
termsvcs           TermService
swprv              swprv
wsappx             WSService,AppXSvc,clipsvc
smphost            smphost
ICService          vmicheartbeat,vmicrdv
LocalServiceNetworkRestricted
eventlog,AudioSrv,wscsvc,LmHosts,AppIDSvc,DHCP,homegroupprovider,wcmsvc,NgcCtnrSvc,i
cssvc,vmictimesync
LocalServicePeerNet PNRPSvc,p2pimsvc,p2psvc,PnrpAutoReg
NetworkServiceAndNoImpersonation KtmRm

wcssvc             WcsPlugInService
appmodel           StateRepository,WalletService,TileDataModelSvc,EntAppSvc
wswpnservice       WpnService
NetworkServiceNetworkRestricted PolicyAgent

AxInstSVGroup      AxInstSV
AppReadiness       AppReadiness
NetworkService
CryptSvc,nlasvc,lanmanworkstation,WinRM,WECSVC,MapsBroker,DNSCache,DHCP,TermService,
Tapisrv

Page 152

```
                        SOFTWARE OUTPUT.txt
UnistackSvcGroup UserDataSvc,PimIndexMaintenanceSvc,UnistoreSvc,OneSyncSvc
print          PrintNotify
------------------------------------------
Launching tracing v.20120509
Microsoft\Tracing
Thu Aug 13 21:54:53 2015   DllHost_RASAPI32
Tue Mar 29 09:31:16 2016   DllHost_RASDLG
Tue Mar 29 09:31:16 2016   DllHost_RASMANCS
Tue Mar 29 09:19:07 2016   Explorer_RASDLG
Tue Mar 29 09:21:57 2016   Explorer_RASGCW
Tue Mar 22 13:30:27 2016   HTTP2GA_RASAPI32
Tue Mar 22 13:30:30 2016   HTTP2GA_RASMANCS
Thu Aug 13 23:03:24 2015   IASMIGPLUGIN_AUX
Wed Mar 23 10:11:13 2016   InstallHMAVPN_RASAPI32
Wed Mar 23 10:11:13 2016   InstallHMAVPN_RASMANCS
Fri Jul 10 11:05:11 2015   IpHlpSvc
Fri Apr  1 22:04:35 2016   LiveUpdateAgent_RASAPI32
Fri Apr  1 22:04:35 2016   LiveUpdateAgent_RASMANCS
Tue Mar 22 13:28:57 2016   LiveUpdateChecker_RASAPI32
Tue Mar 22 13:28:57 2016   LiveUpdateChecker_RASMANCS
Tue Mar 22 10:59:03 2016   McCBEntAndInstru_RASAPI32
Tue Mar 22 10:55:17 2016   mchost_RASAPI32
Tue Mar 22 10:58:48 2016   mcinfo_RASAPI32
Wed Mar 23 11:35:05 2016   McInfo_RASMANCS
Tue Mar 22 10:59:08 2016   McInstru_RASAPI32
Tue Mar 22 11:35:02 2016   McPartnerSAInstallManager_RASAPI32
Tue Mar 22 10:58:58 2016   McPltCmd_RASAPI32
Wed Mar 23 11:28:51 2016   McPltCmd_RASMANCS
Tue Mar 22 10:59:06 2016   McSmtFwk_RASAPI32
Wed Mar 23 12:03:24 2016   McSmtFwk_RASMANCS
Tue Mar 22 13:18:44 2016   McSvHost_RASAPI32
Tue Mar 22 13:18:44 2016   mcsync_RASAPI32
Wed Mar 23 11:35:22 2016   McSync_RASMANCS
Tue Mar 22 10:54:30 2016   McUICnt_RASAPI32
Tue Mar 22 10:55:52 2016   mcupdatemgr_RASAPI32
Tue Mar 22 11:34:47 2016   mcupdate_RASAPI32
Tue Mar 22 10:56:04 2016   MCUPDA~1_RASAPI32
Wed Mar 23 11:58:00 2016   MCUPDA~1_RASMANCS
Tue Mar 22 10:58:54 2016   mcupdutl_RASAPI32
Wed Mar 23 11:58:58 2016   mcupdutl_RASMANCS
Wed Mar 23 10:13:27 2016   MPRAPI
Tue Mar 22 12:53:48 2016   NetworkUXBroker_RASAPI32
Wed Mar 23 10:16:55 2016   NetworkUXBroker_RASMANCS
Wed Mar 23 10:11:33 2016   RASEAP
Wed Mar 23 10:11:33 2016   RASIPHLP
Wed Mar 23 10:11:16 2016   RASMAN
Fri Jul 10 12:21:55 2015   RASPLAP
Wed Mar 23 10:11:33 2016   RASTAPI
Wed Mar 23 10:11:33 2016   svchost_RASAPI32
Wed Mar 23 10:11:33 2016   svchost_RASCHAP
Tue Mar 22 12:53:47 2016   svchost_RASDLG
Wed Mar 23 10:11:33 2016   svchost_RASMANCS
Wed Mar 23 10:11:33 2016   VPNIKE

Wow6432Node\Microsoft\Tracing
Tue Mar 22 12:15:53 2016   abDocsDllLoader_RASAPI32
Tue Mar 22 12:15:53 2016   abDocsDllLoader_RASMANCS
Thu Jul 16 03:44:54 2015   Catalyst_RASAPI32
Tue Mar 22 13:10:52 2016   DashlaneDownloader_RASAPI32
Tue Mar 22 13:10:52 2016   DashlaneDownloader_RASMANCS
Wed Mar 23 10:12:46 2016   HMA! Pro VPN_RASAPI32
Wed Mar 23 10:12:46 2016   HMA! Pro VPN_RASMANCS
Fri Jul 10 11:05:08 2015   IpHlpSvc
                        Page 153
```

```
                          SOFTWARE OUTPUT.txt
Tue Mar 22 11:19:16 2016    McItInfo_RASAPI32
Thu Mar 24 11:58:53 2016    MPRAPI


-----------------------------------------
uninstall v.20140512
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT
hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

Thu Mar 31 18:39:23 2016 (UTC)
  Microsoft Office Office 64-bit Components 2007 v.12.0.6612.1000

Sun Mar 27 13:05:51 2016 (UTC)
  Malwarebytes Anti-Exploit version 1.8.1.1189 v.1.8.1.1189

Sun Mar 27 12:32:21 2016 (UTC)
  Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007 v.12.0.6612.1000

Sun Mar 27 12:32:04 2016 (UTC)
  Microsoft Office Shared 64-bit MUI (English) 2007 v.12.0.6612.1000

Fri Mar 25 12:28:54 2016 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161

Fri Mar 25 12:28:14 2016 (UTC)
  Microsoft Visual C++ 2010  x64 Redistributable - 10.0.30319 v.10.0.30319

Wed Mar 23 09:42:47 2016 (UTC)
  Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000

Thu Aug 13 22:37:26 2015 (UTC)
  Acer Power Management v.7.00.8109

Thu Aug 13 22:35:59 2015 (UTC)
  Acer Explorer Agent v.2.00.3001

Thu Aug 13 22:35:41 2015 (UTC)
  Acer Quick Access v.2.00.3005

Thu Aug 13 22:28:13 2015 (UTC)
  ELAN HIDI2C Filter Driver X64 13.6.3.1_WHQL v.13.6.3.1

Thu Aug 13 22:24:41 2015 (UTC)
  Qualcomm Atheros Bluetooth Suite (64) v.10.0.1.0

Thu Aug 13 22:24:10 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 v.9.0.30729

Thu Aug 13 22:17:27 2015 (UTC)
  Intel(R) Serial IO v.604.10135.1001.55518

Thu Aug 13 22:17:26 2015 (UTC)
  Intel(R) Serial IO v.99.16.55518

Thu Aug 13 22:16:14 2015 (UTC)
  Intel(R) Chipset Device Software v.10.1.1.8

Thu Aug 13 22:15:47 2015 (UTC)
   DriverSetupUtility v.1.00.3011

Thu Aug 13 22:15:02 2015 (UTC)
                          Page 154
```

SOFTWARE OUTPUT.txt
    Intel(R) Trusted Execution Engine v.1.1.1.1

Thu Aug 13 22:14:58 2015 (UTC)
    Intel(R) Trusted Execution Engine v.1.0.0.1064

Thu Aug 13 22:14:57 2015 (UTC)
    Intel(R) Trusted Execution Engine Driver v.1.0.0.1064

Thu Aug 13 21:54:56 2015 (UTC)
    Avast SecureLine v.1.0.239.4

Thu Jul 16 03:47:02 2015 (UTC)
    Acer UEIP Framework v.2.01.3002

Thu Jul 16 03:44:02 2015 (UTC)
    Acer Care Center v.2.00.3005

Fri Jul 10 11:05:48 2015 (UTC)
    AddressBook
    Connection Manager
    DirectDrawEx
    DXM_Runtime
    Fontcore
    IE40
    IE4Data
    IE5BAKEX
    IEData
    MobileOptionPack
    MPlayer2
    SchedulingAgent
    WIC

Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Thu Apr 21 03:27:57 2016 (UTC)
    Java Auto Updater v.2.8.91.14

Thu Apr 21 03:27:18 2016 (UTC)
    Java 8 Update 91 v.8.0.910.14

Thu Apr 21 03:17:41 2016 (UTC)
    McAfee Total Protection v.14.0.8185

Thu Apr 21 03:15:41 2016 (UTC)
    McAfee WebAdvisor v.4.0.187

Fri Apr 15 03:28:04 2016 (UTC)
    Update for Microsoft Office 2007 suites (KB2596787) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2881067) 32-Bit Edition
    Security Update for Microsoft Office PowerPoint 2007 (KB2596912) 32-Bit Edition
    Security Update for Microsoft Office OneNote 2007 (KB2889915) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2596871) 32-Bit Edition
    Security Update for Microsoft Office Word 2007 (KB3114983) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2597969) 32-Bit Edition
    Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB3114982)
32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2760591) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB3114742) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2880507) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2956110) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2880508) 32-Bit Edition
    Security Update for Microsoft Office 2007 suites (KB2850022) 32-Bit Edition
    Microsoft Office 2007 Service Pack 3 (SP3)
                            Page 155

SOFTWARE OUTPUT.txt
Update for Microsoft Office 2007 suites (KB2965286) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2760585) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB3085549) 32-Bit Edition
Security Update for Microsoft Office InfoPath 2007 (KB2687440) 32-Bit Edition
Update for Microsoft Office 2007 suites (KB2596620) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2687409) 32-Bit Edition
Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB3114895)
32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2596754) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2596825) 32-Bit Edition
Security Update for Microsoft Office PowerPoint 2007 (KB3114429) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2825645) 32-Bit Edition
Update for 2007 Microsoft Office System (KB967642)
Security Update for Microsoft Office Excel 2007 (KB3114892) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2596650) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2596792) 32-Bit Edition
Update for Microsoft Office 2007 suites (KB2767916) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB3114542) 32-Bit Edition
Security Update for Microsoft Office 2007 suites (KB2881069) 32-Bit Edition

Fri Apr 15 03:28:02 2016 (UTC)
Microsoft Office Home and Student 2007 v.12.0.6612.1000

Fri Apr 15 03:21:45 2016 (UTC)
Microsoft Office File Validation Add-In v.14.0.5130.5003

Tue Apr 12 20:56:53 2016 (UTC)
Yahoo! Software Update

Tue Apr 12 20:56:45 2016 (UTC)
Yahoo! Toolbar
Yahoo! Toolbar

Tue Apr 12 20:56:21 2016 (UTC)
Yahoo! Messenger

Tue Apr 12 20:55:49 2016 (UTC)
Microsoft Visual C++ 2005 Redistributable v.8.0.61001

Tue Apr 12 20:48:42 2016 (UTC)
Mozilla Firefox 45.0.2 (x86 en-US) v.45.0.2

Tue Apr 12 20:48:36 2016 (UTC)
Mozilla Maintenance Service v.45.0.2.5941

Mon Apr  4 23:33:46 2016 (UTC)
Adobe Flash Player 21 NPAPI v.21.0.0.197

Thu Mar 31 18:39:24 2016 (UTC)
Microsoft Office 2007 Service Pack 3 (SP3)
Security Update for Microsoft Office 2007 suites (KB2825645) 32-Bit Edition

Thu Mar 31 18:27:48 2016 (UTC)
Microsoft Office Shared MUI (English) 2007 v.12.0.6612.1000
Update for Microsoft Office 2007 suites (KB2596787) 32-Bit Edition
Microsoft Office 2007 Service Pack 3 (SP3)
Update for Microsoft Office 2007 Help for Common Features (KB963673)
Update for Microsoft Office Script Editor Help (KB963671)
Security Update for Microsoft Office 2007 suites (KB3085620) 32-Bit Edition

Sun Mar 27 12:35:57 2016 (UTC)
Microsoft Office Proof (French) 2007 v.12.0.6612.1000
Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)
Page 156

SOFTWARE OUTPUT.txt

Sun Mar 27 12:35:53 2016 (UTC)
   Microsoft Office Proof (Spanish) 2007 v.12.0.6612.1000
   Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)

Sun Mar 27 12:35:50 2016 (UTC)
   Microsoft Office Proof (English) 2007 v.12.0.6612.1000
   Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)

Sun Mar 27 12:34:13 2016 (UTC)
   Microsoft Office Home and Student 2007 v.12.0.6612.1000

Sun Mar 27 12:32:52 2016 (UTC)
   Update for Microsoft Office Word 2007 Help (KB963665)
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:51 2016 (UTC)
   Microsoft Office Word MUI (English) 2007 v.12.0.6612.1000

Sun Mar 27 12:32:47 2016 (UTC)
   Microsoft Office PowerPoint MUI (English) 2007 v.12.0.6612.1000
   Update for Microsoft Office Powerpoint 2007 Help (KB963669)
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:41 2016 (UTC)
   Microsoft Office OneNote MUI (English) 2007 v.12.0.6612.1000
   Update for Microsoft Office OneNote 2007 Help (KB963670)
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:30 2016 (UTC)
   Microsoft Office Excel MUI (English) 2007 v.12.0.6612.1000
   Update for Microsoft Office Excel 2007 Help (KB963678)
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:22 2016 (UTC)
   Microsoft Office Shared Setup Metadata MUI (English) 2007 v.12.0.6612.1000
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:21 2016 (UTC)
   Microsoft Office 2007 Service Pack 3 (SP3)

Sun Mar 27 12:32:04 2016 (UTC)
   Microsoft Office 2007 Service Pack 3 (SP3)

Fri Mar 25 12:29:23 2016 (UTC)
   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 v.9.0.30729.6161

Fri Mar 25 12:28:44 2016 (UTC)
   Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319 v.10.0.30319
   {196BB40D-1578-3D01-B289-BEFC77A11A1E}.KB2151757
   {196BB40D-1578-3D01-B289-BEFC77A11A1E}.KB982573

Fri Mar 25 12:28:14 2016 (UTC)
   {DA5E371C-6333-3D8A-93A4-6FD5B20BCC6E}.KB2151757
   {DA5E371C-6333-3D8A-93A4-6FD5B20BCC6E}.KB982573

Wed Mar 23 10:30:27 2016 (UTC)
   Adobe Shockwave Player 12.2 v.12.2.4.194
   swMSM v.12.0.0.1

Wed Mar 23 10:12:00 2016 (UTC)
   HMA! Pro VPN 2.8.24.0 v.2.8.24.0

Page 157

SOFTWARE OUTPUT.txt

Wed Mar 23 09:43:13 2016 (UTC)
  Brother MFL-Pro Suite MFC-9340CDW v.1.0.1.0

Tue Mar 22 13:31:03 2016 (UTC)
  Acer Portal v.3.09.2002

Tue Mar 22 13:27:24 2016 (UTC)
  abPhoto v.3.06.2000.22

Tue Mar 22 13:20:55 2016 (UTC)
  AOP Framework v.3.13.2000.0

Tue Mar 22 13:15:42 2016 (UTC)
  Intel(R) Processor Graphics v.10.18.10.4276

Tue Mar 22 13:15:31 2016 (UTC)
  eBay Worldwide v.2.5.0427

Tue Mar 22 11:54:21 2016 (UTC)
  Malwarebytes Anti-Malware version 2.2.1.1043 v.2.2.1.1043

Tue Mar 22 11:04:51 2016 (UTC)
  Adobe Photoshop Elements 2.0 v.2.0

Tue Mar 22 10:50:30 2016 (UTC)
  Hoyle Puzzle and Board Games 2011 (remove only)

Tue Mar 22 10:34:35 2016 (UTC)
  Microsoft Office Proofing (English) 2007 v.12.0.4518.1014

Thu Aug 13 22:39:54 2015 (UTC)
  Foxit PhantomPDF v.7.0.410.326

Thu Aug 13 22:39:22 2015 (UTC)
  CyberLink PowerDVD 12 v.12.0.4609.02

Thu Aug 13 22:39:21 2015 (UTC)
  InstallShield Uninstall Information

Thu Aug 13 22:39:08 2015 (UTC)
  CyberLink PowerDVD 12 v.12.0.4609.02

Thu Aug 13 22:38:15 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148

Thu Aug 13 22:34:07 2015 (UTC)
  Dashlane Upgrade Service v.1.0.13.0
  {A26EA9EF-0420-4657-AD7F-A4C9D67B63B6}

Thu Aug 13 22:31:05 2015 (UTC)
  Realtek High Definition Audio Driver v.6.0.1.7503

Thu Aug 13 22:28:57 2015 (UTC)
  Realtek Card Reader v.6.3.9600.31213

Thu Aug 13 22:27:37 2015 (UTC)
  Realtek Ethernet Controller Driver v.10.1.505.2015

Thu Aug 13 22:25:24 2015 (UTC)
  Qualcomm Atheros WLAN and Bluetooth Client Installation Program v.12.65

Thu Aug 13 22:24:07 2015 (UTC)
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 v.9.0.30729
                              Page 158

SOFTWARE OUTPUT.txt

Thu Aug 13 22:16:14 2015 (UTC)
  Intel(R) Chipset Device Software v.10.1.1.8

Thu Aug 13 21:54:57 2015 (UTC)
  Game Explorer Categories - genres v.13.0.0.6
  Game Explorer Categories - main v.13.0.0.6
  Dino Storm v.13.0.0.6
  Vegas World v.13.0.0.6
  Villagers and Heroes v.13.0.0.6
  Update Installer for WildTangent Games App
  WildTangent Games App v.4.0.11.16

Thu Jul 16 03:45:59 2015 (UTC)
  WildTangent Games v.1.0.4.0

Thu Jul 16 03:45:57 2015 (UTC)
  12 Labours of Hercules III: Girl Power v.3.0.2.118

Thu Jul 16 03:45:50 2015 (UTC)
  Runefall v.3.0.2.126

Thu Jul 16 03:45:46 2015 (UTC)
  Rory's Restaurant v.3.0.2.126

Thu Jul 16 03:45:42 2015 (UTC)
  Polar Bowler 1st Frame v.3.0.2.59

Thu Jul 16 03:45:40 2015 (UTC)
  Magic Academy v.2.2.0.97

Thu Jul 16 03:45:36 2015 (UTC)
  Jewel Match Snowscapes v.3.0.2.118

Thu Jul 16 03:45:31 2015 (UTC)
  Jewel Match 3 v.2.2.0.97

Thu Jul 16 03:45:12 2015 (UTC)
  Home Makeover v.3.0.2.59

Fri Jul 10 11:05:46 2015 (UTC)
  AddressBook
  Connection Manager
  DirectDrawEx
  DXM_Runtime
  Fontcore
  IE40
  IE4Data
  IE5BAKEX
  IEData
  MobileOptionPack
  MPlayer2
  SchedulingAgent
  WIC

-----------------------------------------
urlzone v.20090526
(Software) URLZONE detection

Microsoft\Windows\CurrentVersion\Internet Settings\urlzone not found.
Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userinit.exe not found.
-----------------------------------------
                        Page 159

SOFTWARE OUTPUT.txt

uac v.20130213
(Software) Get Select User Account Control (UAC) Values from
HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem

UAC Information
Microsoft\Windows\CurrentVersion\policies\system
LastWrite Time Fri Jul 10 12:20:58 2015 (UTC)

EnableLUA value = 1

User Account Control: Run all administrators in Admin Approval Mode
0 = Disabled
1 = Enabled (Default)

EnableVirtualization value = 1

User Account Control: Virtualize file and registry write failures to per-user
locations
0 = Disabled
1 = Enabled (Default)

FilterAdministratorToken value = 0

User Account Control: Admin Approval Mode for the built-in Administrator account
0 = Disabled (Default)
1 = Enabled

ConsentPromptBehaviorAdmin value = 5

User Account Control: Behavior of the elevation prompt for administrators in Admin
Approval Mode
0 = Elevate without prompting
1 = Prompt for credentials on the secure desktop
2 = Prompt for consent on the secure desktop
3 = Prompt for credentials
4 = Prompt for consent
5 = Prompt for consent for non-Windows binaries (Default)

ConsentPromptBehaviorUser value = 3

User Account Control: Behavior of the elevation prompt for standard users
0 = Automatically deny elevation requests
1 = Prompt for consent on the secure desktop
3 = Prompt for consent on the secure desktop (Default)

----------------------------------------
virut v.20130425
(Software) Detect Virut artifacts

Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time Thu Apr 21 03:15:17 2016 (UTC)

UpdateHost value not found.

Also be sure to check the SYSTEM\ControlSet00n\Services\SharedAccess\
Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List key
for exceptions added to the firewall; use the fw_config.pl plugin.
----------------------------------------
win_cv v.20090312
(Software) Get & display the contents of the Windows\CurrentVersion key

Microsoft\Windows\CurrentVersion
LastWrite Time Fri Mar 25 12:34:08 2016 (UTC)

Page 160

SOFTWARE OUTPUT.txt

```
    SM_GamesName : Games
    ProgramFilesPath : %ProgramFiles%
    ProgramFilesDir : C:\Program Files
    DevicePath : %SystemRoot%\inf
    ProgramW6432Dir : C:\Program Files
    MediaPathUnexpanded : %SystemRoot%\Media
    ProgramFilesDir (x86) : C:\Program Files (x86)
    CommonFilesDir : C:\Program Files\Common Files
    CommonW6432Dir : C:\Program Files\Common Files
    SM_ConfigureProgramsName : Set Program Access and Defaults
    CommonFilesDir (x86) : C:\Program Files (x86)\Common Files
----------------------------------------
winbackup v.20120812
(Software) Get Windows Backup

Microsoft\Windows\CurrentVersion\WindowsBackup\ScheduleParams\TargetDevice not
found.

Microsoft\Windows\CurrentVersion\WindowsBackup\Status not found.
----------------------------------------
winlogon v.20130425
(Software) Get values from the WinLogon key

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Apr 21 04:41:14 2016 (UTC)
    LegalNoticeCaption =
    LegalNoticeText =
    AutoRestartShell = 1
    DisableBackButton = 1
    EnableSIHostIntegration = 1
    ForceUnlockLogon = 0
    PasswordExpiryWarning = 5
    PowerdownAfterShutdown = 0
    ReportBootOk = 1
    ShellCritical = 0
    SiHostCritical = 0
    WinStationsDisabled = 0
    scremoveoption = 0
    DisableCAD = 1
    EnableFirstLogonAnimation = 1
    AutoAdminLogon = 0
    IsConnectedAutoLogon = 0
    DisableLockWorkstation = 0
    CachedLogonsCount = 10
    DebugServerCommand = no
    ShutdownFlags = 106
    Background = 0 0 0
    LastUsedUsername = DeputyGod
    DefaultUserName = DeputyGod
    ShellInfrastructure = sihost.exe
    Shell = explorer.exe
    Userinit = C:\Windows\system32\userinit.exe,
    PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    VMApplet = SystemPropertiesPerformance.exe /pagefile
    AutoLogonSID = S-1-5-21-670634337-3447264720-4152838973-1001

Notify subkey not found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Tue Mar 22 12:16:09 2016 (UTC)
    DefaultDomainName =
    DefaultUserName =
```

Page 161

SOFTWARE OUTPUT.txt
```
EnableSIHostIntegration = 1
ShellCritical = 0
SiHostCritical = 0
Shell = explorer.exe
Userinit = C:\Windows\system32\userinit.exe,
PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
```

Notify subkey not found.

Analysis Tips: The UserInit and Shell values are executed when a user logs on.
The UserInit value should contain a reference to userinit.exe; the Shell value
should contain just 'explorer.exe'. Check TaskMan & System values, if found.

Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList not found.
-------------------------------------------
winnt_cv v.20080609
(Software) Get & display the contents of the Windows NT\CurrentVersion key

WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Thu Apr 21 03:19:00 2016 (UTC)

```
    RegisteredOrganization :
    CurrentMinorVersionNumber : 0
    CurrentMajorVersionNumber : 10
    BuildBranch : th1
    CurrentVersion : 6.3
    EditionID : Core
    CurrentBuild : 10240
    UBR : 16771
    CurrentBuildNumber : 10240
    InstallationType : Client
    SoftwareType : System
    InstallTime : H•£õ;Ñ
    RegisteredOwner : DeputyGod
    SystemRoot : C:\Windows
    PathName : C:\Windows
    Customizations : ModernApps
    ProductName : Windows 10 Home
    CurrentType : Multiprocessor Free
    ProductId : 00325-80087-25418-AAOEM
    BuildLab : 10240.th1_st1.160222-1812
    InstallDate : Tue Mar 22 13:08:42 2016 (UTC)
    BuildGUID : ffffffff-ffff-ffff-ffff-ffffffffffff
    BuildLabEx : 10240.16724.amd64fre.th1_st1.160222-1812
    DigitalProductId : a4 00 00 00 03 00 00 00 30 30 33 32 35 2d 38 30 30 38 37 2d 32
35 34 31 38 2d 41 41 4f 45 4d 00 ba 0c 00 00 5b 54 48 5d 58 31 39 2d 39 39 35 32 33
00 00 00 ba 0c a0 3a 52 08 18 4c f7 33 95 60 f6 58 09 00 00 00 00 00 6e 3f f2 55 4c
4e d7 cb 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c7
18 48 78
    DigitalProductId4 : f8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00 2d 00 30
00 33 00 32 00 35 00 38 00 2d 00 30 00 30 00 38 00 2d 00 37 00 32 00 35 00 34 00 31
00 38 00 2d 00 30 00 32 00 2d 00 31 00 30 00 33 00 33 00 2d 00 31 00 30 00 32 00 34
00 30 00 2e 00 30 00 30 00 30 00 30 00 2d 00 32 00 35 00 34 00 32 00 30 00 31 00 35
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 30 00 35 00 36 00 37 00 30 00 37 00 33 00 61 00 2d 00 37 00 64 00 37 00 34
00 2d 00 34 00 30 00 33 00 62 00 2d 00 62 00 32 00 64 00 35 00 2d 00 36 00 62 00 33
00 35 00 64 00 61 00 33 00 37 00 32 00 64 00 38 00 64 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 43 00 6f 00 72 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```
Page 162
```

SOFTWARE OUTPUT.txt

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 ba 0c a0 3a 52 08 18 4c f7 33 95 60 f6 58 09 00 c4 db 78 e9 14 a1 bc d9 f4
35 92 dc 89 b8 43 27 bb d0 b0 3b 64 ad 09 53 4d 14 58 37 2b ba bf dc aa 87 52 eb f6
1a b8 1e c5 ef eb 05 bd 30 1b ce 70 ef a0 3a 14 ea 60 12 eb 15 41 e2 79 f0 b7 7f 5b
00 54 00 48 00 5d 00 58 00 31 00 39 00 2d 00 39 00 39 00 35 00 32 00 33 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 4f 00 45 00 4d 00 3a 00 44 00 4d 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 4f 00 45 00 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```
------------------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Home
InstallDate = Tue Mar 22 13:08:42 2016
------------------------------------------------
yahoo_lm v.20101219
(SOFTWARE) Yahoo Messenger parser

Yahoo not found.
------------------------------------------------
ALERT: user_run: Odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup


ALERT: cmd_shell: Classes\htafile\shell\open\command warning:
C:\Windows\SysWOW64\mshta.exe "%1"
{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}%U{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} %*
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe


Page 163

```
                           SYSTEM OUTPUT.txt
ControlSet001\Control\Session Manager\AppCertDlls not found.
------------------------------------------
appcompatcache v.20140724
(System) Parse files from System hive Shim Cache

Signature: 0x30
Unknown signature: 0x30
------------------------------------------
auditfail v.20081212
(System) Get CrashOnAuditFail value

CrashOnAuditFail = 0
Feature is off; the system will not halt
------------------------------------------
backuprestore v.20130904
(System) Gets the contents of the FilesNotToSnapshot, KeysNotToRestore, and
FilesNotToBackup keys

ControlSet001\Control\BackupRestore\FilesNotToSnapshot
LastWrite Time Fri Jul 10 11:05:06 2015 (UTC)
The listed directories/files are not backed up in Volume Shadow Copies

  WUA : %windir%\softwaredistribution\*.* /s
  OutlookOST : $UserProfile$\AppData\Local\Microsoft\Outlook\*.ost
  FVE : $AllVolumes$\System Volume
Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  FVE2_Wipe : $AllVolumes$\System Volume
Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  FVE2_WipeX : $AllVolumes$\System Volume
Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}.*

FilesNotToBackup key
ControlSet001\Control\BackupRestore\FilesNotToBackup
LastWrite Time Thu Jul 16 03:38:49 2015 (UTC)
Specifies the directories and files that backup applications should not backup or
restore

  Temporary Files : %TEMP%\* /s
  Memory Page File : \Pagefile.sys
  Power Management : \hiberfil.sys
  Netlogon : %SystemRoot%\netlogon.chg
  Internet Explorer : %UserProfile%\index.dat /s
  BITS_LOG : C:\Windows\System32\Bits.log
  BITS_BAK : C:\Windows\System32\Bits.bak
  WUA : %windir%\softwaredistribution\*.* /s
  WER : %ProgramData%\Microsoft\Windows\WER\* /s
  BITS_metadata : C:\ProgramData\Microsoft\Network\Downloader\*
  ETW : %SystemRoot%\system32\LogFiles\WMI\RtBackup\*.*
  Kernel Dumps : %systemroot%\Minidump\* /s %systemroot%\memory.dmp
  Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase
  FVE_Log : \System Volume Information\FVE.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}
  FVE_Wipe : \System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  VSS Default Provider : \System Volume
Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
  VSS Service DB : \System Volume
Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB
  FVE2_Log : \System Volume Information\FVE2.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}
  FVE2_VBB : \System Volume Information\FVE2.{24e6f0ae-6a00-4f73-984b-75ce9942852d}
  FVE2_Wipe : \System Volume Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  VSS Service Alternate DB : \System Volume
Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}ALT
  FVE_Control : \System Volume
Information\FVE.{e40ad34d-dae9-4bc7-95bd-b16218c10f72}.*
                           Page 1
```

SYSTEM OUTPUT.txt

FVE2_Control : \System Volume
Information\FVE2.{e40ad34d-dae9-4bc7-95bd-b16218c10f72}.*
   FVE2_WipeInfo : \System Volume
Information\FVE2.{aff97bac-a69b-45da-aba1-2cfbce434750}.*
   FVE2_WipeX : \System Volume
Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}.*
   MS Distributed Transaction Coordinator : C:\Windows\system32\MSDtc\MSDTC.LOG
C:\Windows\system32\MSDtc\trace\dtctrace.log

KeysNotToRestore key
ControlSet001\Control\BackupRestore\KeysNotToRestore
LastWrite Time Fri Jul 10 11:05:06 2015 (UTC)

Specifies the names of the registry subkeys and values that backup applications
should not restore

   Mount Manager : MountedDevices\
   MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\ASR\
   Session Manager : CurrentControlSet\Control\Session Manager\AllowProtectedRenames
   Pending Rename Operations : CurrentControlSet\Control\Session
Manager\PendingFileRenameOperations
   Pending Rename Operations2 : CurrentControlSet\Control\Session
Manager\PendingFileRenameOperations2
-------------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = LAPTOP-D9R76KLQ
TCP/IP Hostname = LAPTOP-D9R76KLQ
-------------------------------------------
crashcontrol v.20131210
(System) Get crash control information

CrashDumpEnabled = 7 []
DumpFile         = %SystemRoot%\MEMORY.DMP
MinidumpDir      = %SystemRoot%\Minidump
LogEvent         = 1
   Logs an event to the System Event Log (event ID = 1001, source = Save Dump)
-------------------------------------------
ddm v.20081129
(System) Get DDM data from Control Subkey

ControlSet001\Control\DDM not found.
-------------------------------------------
devclass v.20130630
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Fri Sep 11 09:40:59 2015 (UTC)
   Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,05NEOR7OF6IS3C1M&0
Fri Aug 14 02:00:11 2015 (UTC)
   Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,124BWY3VPN6FOX4C&0

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}


-------------------------------------------
disablelastaccess v.20090118
(System) Get NTFSDisableLastAccessUpdate value

Page 2

SYSTEM OUTPUT.txt

```
NtfsDisableLastAccessUpdate
ControlSet001\Control\FileSystem
NtfsDisableLastAccessUpdate = 1
----------------------------------------
dllsearch v.20100824
(System) Get crash control information

dllsearch v.20100824

CWDIllegalInDllSearch value not found.
----------------------------------------
eventlog v.20090112
(System) Get EventLog configuration info


Application \ Thu Apr 21 03:12:51 2016Z
    File              = %SystemRoot%\system32\winevt\Logs\Application.evtx
    DisplayNameFile   = %SystemRoot%\system32\wevtapi.dll
    MaxSize           = 20.00MB
    Retention         = 0 sec
    AutoBackupLogFiles = 0

HardwareEvents \ Fri Jul 10 11:05:05 2015Z
    File              = %systemroot%\system32\winevt\logs\HardwareEvents.evtx
    DisplayNameFile   = %SystemRoot%\system32\wecsvc.dll
    MaxSize           = 20.00MB
    Retention         = 0 sec

Internet Explorer \ Fri Jul 10 11:05:05 2015Z

Key Management Service \ Fri Jul 10 11:05:05 2015Z
    DisplayNameFile   = %SystemRoot%\system32\sppsvc.exe
    MaxSize           = 20.00MB
    Retention         = 0 sec

ODiag \ Tue Mar 22 10:37:05 2016Z
    DisplayNameFile   = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE12\OFFREL.DLL
    MaxSize           = 16.00MB
    Retention         = 0 sec

OSession \ Tue Mar 22 10:37:05 2016Z
    DisplayNameFile   = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE12\OFFREL.DLL
    MaxSize           = 16.00MB
    Retention         = 0 sec

Security \ Thu Jul 16 03:40:55 2015Z
    File              = %SystemRoot%\System32\winevt\Logs\Security.evtx
    DisplayNameFile   = %SystemRoot%\system32\wevtapi.dll
    MaxSize           = 20.00MB
    Retention         = 0 sec

System \ Thu Apr 21 03:10:12 2016Z
    File              = %SystemRoot%\system32\winevt\Logs\System.evtx
    DisplayNameFile   = %SystemRoot%\system32\wevtapi.dll
    MaxSize           = 20.00MB
    Retention         = 0 sec

Windows PowerShell \ Fri Jul 10 11:05:05 2015Z
    MaxSize           = 15.00MB
    Retention         = 0 sec
    AutoBackupLogFiles = 0
```

Page 3

SYSTEM OUTPUT.txt
------------------------------------------
eventlogs v.20081219
(System) Gets Event Log settings from System hive

EventLog Configuration
ControlSet001\Services\Eventlog
LastWrite Time Tue Mar 22 12:21:54 2016 (UTC)
------------------------------------------
fw_config v.20080328
(System) Gets the Windows Firewall config from the System hive

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
LastWrite Time Fri Jul 10 11:05:05 2015 (UTC)
        EnableFirewall -> 1
        DisableNotifications -> 0

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
LastWrite Time Fri Jul 10 11:05:05 2015 (UTC)
        EnableFirewall -> 1
        DisableNotifications -> 0


------------------------------------------
hibernate v.20081216
(System) Check hibernation status

Error reading Heuristics value.
------------------------------------------
ide v.20080418
(System) Get IDE device info from the System hive file

IDE
ControlSet001\Enum\IDE not found.
DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
No IDE subkeys were found.
------------------------------------------
imagedev v.20140104
(System)  --

imagedev
ControlSet001\Control\Class\{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}

Still Image Capture Devices
------------------------------------------
kbdcrash v.20081212
(System) Checks to see if system is config to crash via keyboard

CrashOnCtrlScroll not set
------------------------------------------
legacy v.20120524
(System) Lists LEGACY_* entries in Enum\Root key


------------------------------------------
mountdev v.20130530
(System) Return contents of System hive MountedDevices key


MountedDevices
LastWrite time = Fri Sep 11 09:41:08 2015Z


Page 4

SYSTEM OUTPUT.txt

Device:
_??_USBSTOR#Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100#124BWY3VPN6FOX4C&0#{53f56
307-b6bf-11d0-94f2-00a0c91efb8b}
    \??\Volume{295ec194-4228-11e5-9bd0-806e6f6e6963}

Device:
\??\SCSI#CdRom&Ven_MATSHITA&Prod_DVD-RAM_UJ8HC#4&20be816d&0&010000#{53f5630d-b6bf-11
d0-94f2-00a0c91efb8b}
    \??\Volume{e4d40b53-4205-11e5-9bc8-806e6f6e6963}

Device:
\??\SCSI#CdRom&Ven_HL-DT-ST&Prod_DVDRAM_GUC0N#4&20be816d&0&010000#{53f5630d-b6bf-11d
0-94f2-00a0c91efb8b}
    \DosDevices\E:
    \??\Volume{33951250-5869-11e5-9bd1-806e6f6e6963}

Device: DMIO:ID:G>⌐¿þ⊦K:2┬⌐ô☼w
    \DosDevices\C:

Device:
_??_USBSTOR#Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100#05NEOR7OF6IS3C1M&0#{53f56
307-b6bf-11d0-94f2-00a0c91efb8b}
    \DosDevices\D:
    \??\Volume{33951237-5869-11e5-9bd1-806e6f6e6963}

------------------------------------------
network v.20080324
(System) Gets info from System\Control\Network GUIDs

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}
Interface {0073E1A3-356A-4603-871C-071AB371F75F}
LastWrite time Thu Aug 13 21:56:06 2015 (UTC)
        Name              =
        PnpInstanceID     =
        MediaSubType      =

Interface {090C04E7-9F48-4837-8178-D16205C3EC3C}
LastWrite time Thu Aug 13 22:25:22 2015 (UTC)
        Name              =
        PnpInstanceID     =
        MediaSubType      =

Interface {0DF72CC2-742F-4110-9C16-5C39D814EC49}
LastWrite time Wed Mar 23 10:11:32 2016 (UTC)
        Name              = Local Area Connection* 11
        PnpInstanceID     =
        MediaSubType      =

Interface {26B11A49-585F-4B43-A90C-9AF3C3D7B25B}
LastWrite time Fri Sep 11 09:45:49 2015 (UTC)
        Name              = Local Area Connection* 1
        PnpInstanceID     =
        MediaSubType      =

Interface {28686E81-627C-4392-8326-C58EC38DEA74}
LastWrite time Tue Mar 22 12:53:52 2016 (UTC)
        Name              =
        PnpInstanceID     =
        MediaSubType      =

Interface {30DA98C5-81F4-4459-908B-313297A44B63}
LastWrite time Wed Mar 23 10:11:27 2016 (UTC)
Page 5

```
                              SYSTEM OUTPUT.txt
        Name              = Local Area Connection* 4
        PnpInstanceID     =
        MediaSubType      =

Interface {33042B70-877C-4A24-9695-381005F4A50F}
LastWrite time Thu Apr 21 04:40:59 2016 (UTC)
        Name              = Reusable ISATAP Interface
{33042B70-877C-4A24-9695-381005F4A50F}
        PnpInstanceID     =
        MediaSubType      =

Interface {34E462D0-5729-4F1E-9D8F-252BA198070D}
LastWrite time Wed Mar 23 10:13:28 2016 (UTC)
        Name              = Local Area Connection* 7
        PnpInstanceID     =
        MediaSubType      =

Interface {37D3F9AB-092C-400F-AEE6-CCD2D068D2C0}
LastWrite time Wed Mar 23 10:11:33 2016 (UTC)
        Name              = Local Area Connection* 12
        PnpInstanceID     =
        MediaSubType      =

Interface {4A02EE9B-012C-43FD-B03C-7F88C0F07054}
LastWrite time Thu Aug 13 22:21:56 2015 (UTC)
        Name              =
        PnpInstanceID     =
        MediaSubType      =

Interface {4B70E633-0701-4E68-B498-A30F043E4A29}
LastWrite time Wed Mar 23 10:13:28 2016 (UTC)
        Name              = Local Area Connection* 5
        PnpInstanceID     =
        MediaSubType      =

Interface {4D71E8FB-A8D1-4154-AB9B-D4F5AB63629B}
LastWrite time Wed Mar 23 10:13:28 2016 (UTC)
        Name              = Local Area Connection* 6
        PnpInstanceID     =
        MediaSubType      =

Interface {4F2D51A0-408D-4902-9285-BFE8F42E8708}
LastWrite time Wed Mar 23 10:11:59 2016 (UTC)
        Name              = Ethernet 2
        PnpInstanceID     =
        MediaSubType      =

Interface {4F7B3ED4-3AE9-4AC3-9818-C8B4A574F0BE}
LastWrite time Thu Aug 13 21:56:06 2015 (UTC)
        Name              =
        PnpInstanceID     =
        MediaSubType      =

Interface {59FD0C9E-A658-48B7-95D1-E1F0DBD558C5}
LastWrite time Wed Mar 23 10:11:17 2016 (UTC)
        Name              = Local Area Connection* 3
        PnpInstanceID     =
        MediaSubType      =

Interface {5F09F18B-50C9-4706-A669-10163B1696CD}
LastWrite time Thu Apr 21 04:41:17 2016 (UTC)
        Name              = Reusable ISATAP Interface
{5F09F18B-50C9-4706-A669-10163B1696CD}
                              Page 6
```

```
                              SYSTEM OUTPUT.txt
        PnpInstanceID        =
        MediaSubType         =

Interface {6980ACBD-0534-40B0-B5C1-C4CBCD05902A}
LastWrite time Tue Mar 22 13:06:05 2016 (UTC)
        Name                 = Teredo Tunneling Pseudo-Interface
        PnpInstanceID        =
        MediaSubType         =

Interface {6EB1A476-227C-413B-B485-C8B6469D64D9}
LastWrite time Fri Sep 11 09:45:49 2015 (UTC)
        Name                 = Ethernet
        PnpInstanceID        =
        MediaSubType         =

Interface {6EDCD08C-9DE6-4138-956E-CF9ADDE89BC3}
LastWrite time Fri Sep 11 09:45:49 2015 (UTC)
        Name                 = Wi-Fi
        PnpInstanceID        =
        MediaSubType         = 2

Interface {7693AA39-CA40-44D3-9B0C-5D43394D3BB6}
LastWrite time Wed Mar 23 10:13:28 2016 (UTC)
        Name                 = Bluetooth Network Connection 2
        PnpInstanceID        =
        MediaSubType         = 7

Interface {7DC66641-9D5E-4735-9101-411F817F25C7}
LastWrite time Thu Aug 13 22:21:24 2015 (UTC)
        Name                 =
        PnpInstanceID        =
        MediaSubType         =

Interface {8466E0C9-9915-4852-8102-E3DC25A935C3}
LastWrite time Wed Mar 23 10:11:14 2016 (UTC)
        Name                 = Local Area Connection* 2
        PnpInstanceID        =
        MediaSubType         =

Interface {871BD6EF-F398-4B20-B59F-2F1405BE5422}
LastWrite time Wed Mar 23 10:11:28 2016 (UTC)
        Name                 = Local Area Connection* 8
        PnpInstanceID        =
        MediaSubType         =

Interface {8CF0274F-5831-4D0F-A05B-28C2F9DF2F54}
LastWrite time Wed Mar 23 10:11:31 2016 (UTC)
        Name                 = Local Area Connection* 10
        PnpInstanceID        =
        MediaSubType         =

Interface {8FAC2DC4-1983-4021-BE21-75F3FEE1B984}
LastWrite time Thu Aug 13 22:24:50 2015 (UTC)
        Name                 =
        PnpInstanceID        =
        MediaSubType         =

Interface {948BA694-FD68-44BB-86D0-A86F0092738D}
LastWrite time Thu Aug 13 21:56:06 2015 (UTC)
        Name                 =
        PnpInstanceID        =
        MediaSubType         =
```

Page 7

```
                            SYSTEM OUTPUT.txt
Interface {96B2AF69-60CC-41B2-AB64-2CE45FD8FEA8}
LastWrite time Fri Jul 10 12:22:48 2015 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {AE960D9F-2E50-400A-ABBA-EDDC02012C89}
LastWrite time Tue Mar 22 12:53:52 2016 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {B59082F0-E054-4477-9F42-0611D83208AB}
LastWrite time Tue Mar 22 12:53:52 2016 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {C95A6B67-4DC0-4FD5-A93B-4FF571599E39}
LastWrite time Wed Mar 23 10:11:59 2016 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {DD75F478-24D5-4C5E-B1CA-8A284D2EFDE8}
LastWrite time Thu Aug 13 21:56:06 2015 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {E46D29B2-D7FC-482F-81BA-F2BBDD1BF56C}
LastWrite time Thu Aug 13 22:24:37 2015 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

Interface {E9E1094C-C5C2-47AD-BD99-7B2243A2FAD0}
LastWrite time Wed Mar 23 10:11:29 2016 (UTC)
        Name            = Local Area Connection* 9
        PnpInstanceID   =
        MediaSubType    =

Interface {F0F2C058-40EA-40BC-AF87-5459AF2E2425}
LastWrite time Wed Mar 23 10:13:28 2016 (UTC)
        Name            = Wi-Fi 2
        PnpInstanceID   =
        MediaSubType    = 2

Interface {FC0C80B2-B569-4C57-BE49-5273B20D37C3}
LastWrite time Thu Aug 13 21:56:06 2015 (UTC)
        Name            =
        PnpInstanceID   =
        MediaSubType    =

-------------------------------------
nic v.20100401
(System) Gets NIC info from System hive

-------------------------------------
nic_mst2 v.20080324
(System) Gets NICs from System hive; looks for MediaType = 2

Network key
```

SYSTEM OUTPUT.txt
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

No active network interface cards were found.
------------------------------------------
nic2 v.20100401
(System) Gets NIC info from System hive

Adapter: {26b11a49-585f-4b43-a90c-9af3c3d7b25b}
LastWrite Time: Fri Jul 10 12:20:51 2015 Z
    EnableDHCP                    1
    Domain
    NameServer

Adapter: {34e462d0-5729-4f1e-9d8f-252ba198070d}
LastWrite Time: Fri Sep 11 09:42:27 2015 Z
    EnableDHCP                    1
    Domain
    NameServer

Adapter: {4d71e8fb-a8d1-4154-ab9b-d4f5ab63629b}
LastWrite Time: Fri Sep 11 09:42:25 2015 Z
    EnableDHCP                    1
    Domain
    NameServer

Adapter: {4f2d51a0-408d-4902-9285-bfe8f42e8708}
LastWrite Time: Thu Apr 21 04:40:58 2016 Z
    EnableDHCP                    1
    Domain
    NameServer
    DhcpIPAddress                0.0.0.0
    DhcpSubnetMask               255.0.0.0
    DhcpServer                   255.255.255.255
    Lease                        31536000
    LeaseObtainedTime            Thu Apr 21 03:29:42 2016 Z
    T1                           Thu Oct 20 15:29:42 2016 Z
    T2                           Mon Mar  6 12:29:42 2017 Z
    LeaseTerminatesTime          Fri Apr 21 03:29:42 2017 Z
    AddressType                  0
    IsServerNapAware             0
    DhcpConnForceBroadcastFlag   0
    DhcpInterfaceOptions         ü              ÚY↑W/          ÚY↑W.
    ÚY↑W,              ÚY↑W+           ÚY↑W!          ÚY↑W
ÚY↑Wÿ            ÚY↑WL           ÚY↑W–          ÚY↑W          ÚY↑W3
            ÚY↑W6           ÚY↑W5          ÚY↑W

Adapter: {6bb4f047-2706-11e5-9bbe-806e6f6e6963}
LastWrite Time: Fri Jul 10 12:21:43 2015 Z

Adapter: {6eb1a476-227c-413b-b485-c8b6469d64d9}
LastWrite Time: Thu Aug 13 21:56:06 2015 Z
    EnableDHCP                    1
    Domain
    NameServer

Adapter: {6edcd08c-9de6-4138-956e-cf9adde89bc3}
LastWrite Time: Thu Aug 13 21:56:11 2015 Z
    EnableDHCP                    1
    Domain
    NameServer

Adapter: {7693aa39-ca40-44d3-9b0c-5d43394d3bb6}
LastWrite Time: Fri Sep 11 09:41:39 2015 Z

Page 9

```
                         SYSTEM OUTPUT.txt
    EnableDHCP                  1
    Domain
    NameServer

Adapter: {f0f2c058-40ea-40bc-af87-5459af2e2425}
LastWrite Time: Thu Apr 21 03:19:17 2016 Z
    EnableDHCP                  1
    Domain
    NameServer
    DhcpIPAddress              192.168.1.237
    DhcpSubnetMask             255.255.255.0
    DhcpServer                 192.168.1.1
    Lease                      86400
    LeaseObtainedTime          Thu Apr 21 03:19:17 2016 Z
    T1                         Thu Apr 21 15:19:17 2016 Z
    T2                         Fri Apr 22 00:19:17 2016 Z
    LeaseTerminatesTime        Fri Apr 22 03:19:17 2016 Z
    AddressType                0
    IsServerNapAware           0
    DhcpConnForceBroadcastFlag 0
    DhcpNetworkHint            2427164646F636B6
    DhcpDefaultGateway         192.168.1.1
    DhcpNameServer             192.168.1.1
    DhcpSubnetMaskOpt          255.255.255.0
    DhcpInterfaceOptions       y              uï↑W/           uï↑W.
    uï↑W,          uï↑W+         ↵    uï↑W!           uï↑W
uï↑W☼          uï↑W└        5˜╠WÀ¨   ü       ↵          5˜╠W
    Q.      ↑    5˜╠W└ÿÿLAPTOP-D9R76KLQ   -              5˜╠WÀ¨           ↵
5˜╠WÀ¨  ÿ        ↵     5˜╠Wÿÿÿ  ;           ↵    5˜╠W   'P:        ↵      5˜╠W   ¨À3
 ↵     5˜╠W   Q6       ↵    5˜╠WÀ¨   5        5˜╠W|
    DhcpGatewayHardware        À¨  -   à?I{@
    DhcpGatewayHardwareCount   1

---------------------------------------------
nolmhash v.20100712
(System) Gets NoLMHash value

nolmhash v.20100712
ControlSet001\Control\Lsa
LastWrite: Thu Apr 21 03:18:59 2016

NoLMHash value = 1

A value of 1 indicates that LMHashes are not stored in the SAM.
---------------------------------------------
pagefile v.20140505
(System) Get info on pagefile(s)

PagingFiles = ?:\pagefile.sys
ClearPageFileAtShutdown = 0
PagingFiles = ?:\pagefile.sys
---------------------------------------------
prefetch v.20120914
(SYSTEM) Gets the the Prefetch Parameters

EnablePrefetcher    = 3

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled
---------------------------------------------
productpolicy v.20091116
```

Page 10

SYSTEM OUTPUT.txt
(System) Parse ProductPolicy value (Vista & Win2008 ONLY)


Note: This plugin applies to Vista and Windows 2008 ONLY.
For a listing of names and values, see:
http://www.geoffchappell.com/viewer.htm?doc=notes/windows/license/install.htm&tx=3,5
,6;4

4A0C606B-2CE9-4A35-9B3E-A57D37F18632 -
340000000100010001000100020001000000040001000100962b22e922cd840e84bee09d1c4742ba12b9
c81f3e44967dca9ee0a5b4e80236506a9eb8d206203a6e88a2bc
ACLUIFileFolderTool-IsSecurityUIEnabled - 1
AMR-CODECS-MSAMRNBInSKU - 1
AppXDeploymentServer-License-MaxSideloadedPackagesCount - 4294967295
BuildFlighting-ControlBuildFlighting - 0
ChangeDesktopBackground-Enabled - 1
ClipService-EnableLOBApps - 0
ClipService-LOBSideloadingActivated - 0
ContentDeliveryManager-License-ContentDeliveryAllowed - 1
ContentDeliveryManager-License-OemPreInstalledOnUpgradeAllowed - 1
ContentDeliveryManager-License-SoftLandingAllowed - 1
DNS-Client-license-DAPolicy - 0
DolbyDecMFT-DolbyDigitalDecoderV3AddIn - 0
DolbyDecMFT-DolbyDigitalDecoderV3AddInEnable - 1
DolbyDecMFT-DolbyDigitalDecoderV3InSKU - 1
ExtensibleStorageEngine-ISAM-ParamConfiguration - 1
GroupPolicy-License-DomainIncapableSystem - 1
GroupPolicy-License-NetworkWaitTimeoutInSeconds - 30
GroupPolicy-License-WaitForNetwork - 0
HealthAttestationCSP-UseSecTask - 0
IASLicensing-allowSubnetSyntax - 0
IASLicensing-maxClient - 0
IASLicensing-maxServerGroups - 0
Internet-Browser-License-LicensedPartnerID - 0
Kernel-DynamicPartitioningSupported - 0
Kernel-ExpirationDate - 00000000000000000000000000000000
Kernel-Fingerprint-Verification-Disabled - 0
Kernel-MUI-Language-Allowed - EMPTY
Kernel-MUI-Language-Disallowed - EMPTY
Kernel-MUI-Language-SKU -
en-US;en-AU;en-CA;en-GB;en-HK;en-IE;en-NZ;en-SG;ar-SA;pt-BR;zh-TW;zh-CN;zh-HK;zh-SG;
cs-CZ;da-DK;el-GR;es-AR;es-CL;es-CO;es-ES;es-MX;es-US;fi-FI;fr-BE;fr-CA;fr-CH;fr-FR;
de-AT;de-CH;de-DE;he-IL;hu-HU;it-IT;ja-JP;ko-KR;nl-BE;nl-NL;nb-NO;pl-PL;pt-PT;ru-RU;
sv-SE;tr-TR;bg-BG;hr-HR;et-EE;lv-LV;lt-LT;ro-RO;sr-Latn-CS;sr-Latn-RS;sk-SK;sl-SI;th
-TH;uk-UA;fy-NL;qps-ploc;qps-plocm;qps-Latn-x-sh
Kernel-MUI-Number-Allowed - 1000
Kernel-MaxPhysicalPage - 4096
Kernel-MemoryMirroringSupported - 0
Kernel-NativeVHDBoot - 0
Kernel-NonGenuineNotificationStringIds - 113200001202000053060000
Kernel-NonGenuineNotificationType - 2
Kernel-OneCore-DeviceFamilyID - 3
Kernel-PersistDefectiveMemoryList - 0
Kernel-PhysicalMemoryAddAllowed - 0
Kernel-ProductInfo - 101
Kernel-ProductInfoLegacyMapping - 060000000200000000000000000000000003000000
Kernel-RegisteredProcessors - 1
Kernel-VirtualDynamicPartitioningSupported - 0
Kernel-WindowsMaxMemAllowedArm - 4096
Kernel-WindowsMaxMemAllowedArm64 - 131072
Kernel-WindowsMaxMemAllowedx64 - 131072
Kernel-WindowsMaxMemAllowedx86 - 4096
LSA-Policy-DisableBuiltinAdminByDefault - 0

Page 11

```
                              SYSTEM OUTPUT.txt
LSA-Policy-DisableBuiltinGuestByDefault - 0
LSA-Policy-EnableCredentialIsolation - 0
LSA-Policy-EnableTrustedDomains - 0
MF-SLPolicy-HMFTMeritValidationRequired - 1
MF-SLPolicy-PMPSessionInProcess - 0
MF-SLPolicy-SkipOPMVerification - 0
MSAudDecMFT-AACDecoderV3AddIn - 0
MSAudDecMFT-AACDecoderV3AddInEnable - 1
MSAudDecMFT-AACDecoderV3InSKU - 1
MathRecognizerEventsLicensing-EnableMathRecognizer - 1
Microsoft-Windows-Core-AllowMultiMon - 1
Microsoft-Windows-Core-AllowedControlledDevicesForBoot - 12
Microsoft-Windows-Core-NeedsFullOEMVerification - 1
Microsoft-Windows-Core-THQAEnabled - 1
Microsoft-Windows-DOT11PREF-AllowAdhoc - 1
Microsoft-Windows-DesktopWindowManager-Core-AnimatedTransitionsAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-Flip3dAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-LivePreviewAllowed - 1
Microsoft-Windows-DesktopWindowManager-Core-TransparencyAllowed - 1
Microsoft-Windows-Fax-Common-DeviceLimit - 1
Microsoft-Windows-Fax-Common-EnableServerPolicy - 0
Microsoft-Windows-IE-InternetExplorer-SupportEnableAutoUpgrade - 1
Microsoft-Windows-InternetConnectionSharingConfig-HomeNetBeacon - 1
Microsoft-Windows-InternetConnectionSharingConfig-HomeNetICS - 1
Microsoft-Windows-ProximityMessaging-RtApi-App2Device - 0
Microsoft-Windows-ProximityMessaging-RtApi-Reconnect - 0
Microsoft-Windows-ProximityMessaging-RtApi-SubscriptionTracking - 0
Microsoft-Windows-QWAVE-EnableAdaptiveFlow - 1
Microsoft-Windows-QWAVE-Layer3Probing - 1
Microsoft-Windows-SensorsLicense-EnableCPL - 1
MicrosoftWindowsSafeDocsMain-BackupToNetShare - 1
MicrosoftWindowsSafeDocsMain-GPSupport - 1
MicrosoftWindowsSafeDocsMain-PerUserBackup - 1
MobilePCMobilityCenter-EnableMobilityCenter - 1
NetworkProfile-License-CostEnabled - 1
NetworkSecurity-IKE-Kerberos - 1
NetworkSecurity-IKE-LowMemorySystem - 0
NetworkSecurity-IPsecDoSProtection-EnabledPolicy - 0
Networking-MPSSVC-Svc-License-NetIsolationOnly - 0
NlaSvc-Licensing-LANIds-BSSIDRetrieval-Enabled - 1
NlaSvc-Licensing-LANIds-LLDPDriver-Enabled - 0
NlaSvc-Licensing-LANIds-Service-Enabled - 1
OrchestratorUpdateHandlersPolicies-DeferredInstallDisabled - 0
PEAuth-Available - 1
PeerToPeerBase-Graphing-EnabledPolicy - 1
PeerToPeerBase-Grouping-EnabledPolicy - 1
PeerToPeerBase-IdManager-EnabledPolicy - 1
PeerToPeerBase-Pnrp-EnabledPolicy - 1
Personalization-Enabled - 1
PhotoMinFeature-AdvancedSlideshow - 1
PhotoMinFeature-MakeDVD - 1
PickerRestrictedPolicy-Enabled - 0
Printing-Spooler-Core-Localspl-Licensing-Enabled - 1
Printing-Spooler-Core-Spoolss-Licensing-Enabled - 1
Printing-Spooler-Core-Spoolss-Licensing-Network-Default-Printer-Enabled - 0
RasBase-DefaultConnections - 2
RasBase-DisableDialup - 0
RasBase-DisableIsdn - 0
RasBase-DisableRasScript - 0
RasBase-EnableOnDemandDriverLoad - 1
RasBase-MaxConnections - 3
RasBase-RasMobileCore - 0
RetailDemo.License-RetailDemoAllowed - 1
                              Page 12
```

SYSTEM OUTPUT.txt

```
SLC-Component-SKU-OCUR-OCURControlContentAllowed - 0
SMBServer-AllowHashPublication - 0
SMBServer-AllowRemoteLegacyShadowCopyAccess - 0
SMBServer-AllowRemoteShadowCopyAccess - 1
SMBServer-WindowsMaxInSMBConns - 20
SecureStartupFeature-Enabled - 1
SecureStartupFeature-Enabled-DeviceEncryption - 1
SecureStartupFeature-Enabled-DeviceEncryption-BlockRevert - 0
SecureStartupFeature-Enabled-Driver - 1
SecureStartupFeature-Enabled-PreInstall - 0
SecureStartupFeature-Enabled-Premium - 0
SecureStartupFeature-PerfWarning - 0
Security-SPP-Action-StateData -
AppId=55c92734-d682-4d71-983e-d6ec3f16059f;LastConsumptionReason=0x00000000;LastNoti
ficationId=Cleanup;LicenseState=SL_LICENSING_STATUS_LICENSED;PartialProductKey=4X8VD
;ProductKeyType=OEM:DM;SkuId=0567073a-7d74-403b-b2d5-6b35da372d8d;ruleId=379cccfb-d4
e0-48fe-b0f2-0136097be147;uxDifferentiator=OEM_DM
Security-SPP-ActivationResetCount - 1001
Security-SPP-ActivationResetCountMax - 2147483647
Security-SPP-ApplicationActivationResetCount - 1001
Security-SPP-ApplicationActivationResetCountMax - 2147483647
Security-SPP-CMIDExpirationPeriod - 43200
Security-SPP-EvaluationModeEnabled - 0
Security-SPP-GenuineLocalStatus - 1
Security-SPP-IACountedIdList -
Security-SPP-KmsCountedIdList -
Security-SPP-LastWindowsActivationHResult - 00000000
Security-SPP-LastWindowsActivationTime - c148c9263c84d101
Security-SPP-Reserved-IAAuthenticationKey -
o8SSv/EBs8rqhGavBcqlARU9vkhlA8k3uuMw+yJ4euCvhvDB3UKsi8veT8crtfg7VX8ZIGVqCG4OFDm8X9M+
P1ZTTyJWuMBnmcKzf4GNdHmkFdxJ2ZD8KKhN8IOMkM7732jL72Ncr9wLrGY3iflAlWxH/PfW4DlYJFwuJTIg
eJU=
Security-SPP-Reserved-IAAuthenticationKeyTest -
xCF2keDbBzFBBetbNjI5tdcw/3DHcDXmc+VgqFyQmSEnCFLmOSKwKcoVgFj9TOu+2niz45b4p/DZO2CKmOfz
JWHrIobpa77lyh1NAlzCpsuuyIFOgYtHY5CtnmKWu1/z8TiyJEgWWxnHvXQbK+3KTGzLaPrmILejhgO+TJt2
CYA=
Security-SPP-Reserved-SkuPpdConsumed - 1
Security-SPP-Reserved-TBLProductKeyType - 0
Security-SPP-Reserved-TBLRemainingTime - 0
Security-SPP-Reserved-TBLState - 0
Security-SPP-SharedLicense - 0
Security-SPP-TokenActivation-AdditionalInfo -
Security-SPP-WriteWauMarker - 1
SnippingToolLicensing-Enabled - 1
StickyNotesLicensing-Enabled - 1
TabletPC-MathInputLicensing-EnableMathInput - 1
TabletPC-tabbtn-EnableButtons - 1
TabletPCAccessories-EnableJournal - 1
TabletPCAccessories-EnableStickyNotes - 1
TabletPCInputPanel-EnableTIP - 1
TabletPCInputPanel-EnableTIPSynced - 1
TabletPCPlatformInput-core-EnableTouchUI - 1
TabletPCPlatformInput-core-MultiTouchGestures - 1
TabletPCPlatformInput-core-SFP - 1
TelemetryPermission-AllowDisable - 0
TerminalServices-DeviceRedirection-Licenses-PnpRedirectionAllowed - 0
TerminalServices-DeviceRedirection-Licenses-TSAudioCaptureAllowed - 0
TerminalServices-DeviceRedirection-Licenses-TSEasyPrintAllowed - 0
TerminalServices-DeviceRedirection-Licenses-TSMFPluginAllowed - 0
TerminalServices-RDP-7-Advanced-Compression-Allowed - 0
TerminalServices-RemoteConnectionManager-0f0a4bf8-8362-435d-938c-222a518a8b78-Disabl
ed - 1
TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-LocalO
```

Page 13

SYSTEM OUTPUT.txt

```
nly - 1
TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSes
sions - 1
TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-Initia
lProgram - %SystemRoot%\ehome\mcrmgr.exe
TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSes
sions - 0
TerminalServices-RemoteConnectionManager-AllowAppServerMode - 0
TerminalServices-RemoteConnectionManager-AllowD3DRemoting - 0
TerminalServices-RemoteConnectionManager-AllowMultimon - 0
TerminalServices-RemoteConnectionManager-AllowMultipleSessions - 1
TerminalServices-RemoteConnectionManager-AllowRemoteConnections - 0
TerminalServices-RemoteConnectionManager-MaxUserSessions - 0
TerminalServices-RemoteConnectionManager-b7857721-7a62-4a37-aff3-253fe2b8b0e8-MaxSes
sions - 0
TerminalServices-RemoteConnectionManager-ce0ad219-4670-4988-98fb-89b14c2f072b-MaxSes
sions - 1
UpdatePolicy-UpdateManagementGroup - 0
UserOOBE-Allowed-SignIn-Identity - 3
VirtualPC-licensing-Enabled - 0
WMPPlayer-HMEAllowed - 1
WMPPlayer-RMEAllowed - 1
WMPPlayer-RMESecurityGroupAllowed - 0
WSLicensingService-EnableLOBApps - 0
WSLicensingService-LOBSideloadingActivated - 0
WebServices-ListenerApiInAppContainer - 0
Windows.Globalization.License-TextSuggestionApi-DgmlRootName -
ComponentLayoutsDesktop
Windows.Globalization.License-TextSuggestionApi-LangResourcesInstalledByDefault - 1
Windows.Globalization.License-TextSuggestionApi-SupportedLanguagesForConversion -
ja-JP;zh-Hans-CN;
Windows.Globalization.License-TextSuggestionApi-SupportedLanguagesForPrediction -
ja-JP;
Windows.Globalization.License-TextSuggestionApi-SupportedLanguagesForReverseConversi
on - ja-JP;
WindowsAnytimeUpgrade-CanUpgrade - 1
WindowsSearchComponent-ComponentInstalled - 1
WorkstationService-DomainJoinEnabled - 0
appid-EnableV2 - 0
configmanager2-License-BlockedProviderList -
0$activesync;0$assignedaccess;0$bulkenrollment;0$certificatestore;0$clientcertificat
einstall;0$defender;0$devicestatus;0$diagnosticlog;0$dmclient;0$email2;0$enterprisea
pn;0$enterprisedesktopappmanagement;0$enterprisemodernappmanagement;0$nodecache;0$pa
ssportforwork;0$remotefind;0$remotewipe;0$reporting;0$unifiedwritefilter;0$update;0$
vpnv2;0$wifi;0$win32appinventory;
deviceregistration-MaximumUsers - 1
dmenrollengine-Allowed-Enrollments - 9effffffffffffff
dmenrollengine-Mobile-Business - 0
enterprisemgmt_policymanager-License-MDMPolicyAllowList -
AboveLock|Accounts|ApplicationManagement|Authentication|Bluetooth|Browser|Camera|Con
nectivity|DataProtection|Defender|DeliveryOptimization|DeviceLock|Experience|Knobs|R
MS|Search|Security|Settings|Start|System|TextInput|Update|WiFi
explorer-AeroAnimationAllowed - 1
explorer-AeroShakeAllowed - 1
explorer-AlwaysShowRunAsDifferentUser - 0
explorer-ClientLoginExperienceAllowed - 1
feclient-EfsEnabled - 0
feclient-EfsEnabledBasic - 1
feclient-EfsUserCacheLimit - 5
hevcdecoder-HEVCVideoDecoderV1AddIn - 0
hevcdecoder-HEVCVideoDecoderV1AddInEnable - 1
hevcdecoder-HEVCVideoDecoderV1InSKU - 1
iuilp-DefaultLauncherLayoutBase - 0
```

Page 14

```
                          SYSTEM OUTPUT.txt
iuilp-SkipRequiredAppsCheck - 0
msac3enc-DolbyDigitalEncoderV3AddIn - 0
msac3enc-DolbyDigitalEncoderV3AddInEnable - 1
msac3enc-DolbyDigitalEncoderV3InSKU - 1
msmpeg2adec-AACDecoderV2AddIn - 0
msmpeg2adec-AACDecoderV2AddInEnable - 1
msmpeg2adec-AACDecoderV2InSKU - 1
msmpeg2adec-DolbyDigitalDecoderV3AddIn - 0
msmpeg2adec-DolbyDigitalDecoderV3AddInEnable - 1
msmpeg2adec-DolbyDigitalDecoderV3InSKU - 1
msmpeg2enc-MPEG2VideoEncoderV3AddIn - 0
msmpeg2enc-MPEG2VideoEncoderV3AddInEnable - 1
msmpeg2enc-MPEG2VideoEncoderV3InSKU - 0
msmpeg2vdec-H264VideoDecoderV2AddIn - 0
msmpeg2vdec-H264VideoDecoderV2AddInEnable - 1
msmpeg2vdec-H264VideoDecoderV2InSKU - 1
msmpeg2vdec-MPEG2VideoDecoderV3AddIn - 0
msmpeg2vdec-MPEG2VideoDecoderV3AddInEnable - 1
msmpeg2vdec-MPEG2VideoDecoderV3InSKU - 0
msoobe-FirstLogonAnim-MayBeDisabled - 0
parentalcontrols-EnableFeature - 1
provsvc-license-HomeGroupCreate - 1
shell-homegroup-Enabled - 1
shell32-license-GroupPolicy-TryHarderPinned - 0
shell32-license-ShowProductNameOnDesktop - 0
shell32-license-UseBingAsDefaultSearchProvider - 0
transmog-CanTransmogDC - 1
volmgrx-SupportDynamic - 1
volmgrx-SupportMirror - 0
volmgrx-SupportRaid5 - 0
------------------------------------
producttype v.20100325
(System) Queries System hive for Windows Product info

ControlSet001\Control\ProductOptions
LastWrite = Thu Apr 21 03:22:20 2016

Ref: http://support.microsoft.com/kb/152078
     http://support.microsoft.com/kb/181412

ProductType  = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

ProductSuite = Terminal Server Personal
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx
------------------------------------
rdpport v.20100713
(System) Queries System hive for RDP Port

rdpport v.20100713

Remote Desktop Listening Port Number = 3389
------------------------------------
routes v.20100817
(System) Get persistent routes

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
LastWrite: Fri Jul 10 11:05:05 2015

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes has no values.
                          Page 15
```

SYSTEM OUTPUT.txt
------------------------------------------
safeboot v.20081216
(System) Check SafeBoot entries

Minimal   [Thu Apr 21 03:11:17 2016 Z]
Fri Jul 10 11:05:06 2015 Z
  Ahcache.sys (Driver)
  AppInfo (Service)
  AppMgmt (Service)
  Base (Driver Group)
  BasicDisplay.sys (Driver)
  BasicRender.sys (Driver)
  Boot Bus Extender (Driver Group)
  Boot file system (Driver Group)
  BrokerInfrastructure (Service)
  CoreMessagingRegistrar (Service)
  CryptSvc (Service)
  DcomLaunch (Service)
  DeviceInstall (Service)
  dxgkrnl.sys (Driver)
  EFS (Service)
  EventLog (Service)
  File system (Driver Group)
  Filter (Driver Group)
  FsDepends.sys (Driver)
  HelpSvc (Service)
  KeyIso (Service)
  LSM (Service)
  Netlogon (Service)
  NTDS (Service)
  PCI Configuration (Driver Group)
  PlugPlay (Service)
  PNP Filter (Driver Group)
  Power (Service)
  Primary disk (Driver Group)
  ProfSvc (Service)
  RpcEptMapper (Service)
  RpcSs (Service)
  sacsvr (Service)
  SCSI Class (Driver Group)
  sermouse.sys (Driver)
  StateRepository (Service)
  SWPRV (Service)
  System Bus Extender (Driver Group)
  SystemEventsBroker (Service)
  TabletInputService (Service)
  TBS (Service)
  TileDataModelSvc (Service)
  TrustedInstaller (Service)
  UserManager (Service)
  VDS (Service)
  vmms (Service)
  volmgr.sys (Driver)
  volmgrx.sys (Driver)
  WinDefend (Service)
  WinMgmt (Service)
  WudfPf (Driver)
  WudfRd (Driver)
  WudfSvc (Service)
  {36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)
  {4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)
  {4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)
  {4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)
                    Page 16

```
                            SYSTEM OUTPUT.txt
    {4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)
    {4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)
    {4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)
    {4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)
    {4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)
    {4D36E97D-E325-11CE-BFC1-08002BE10318} (System)
    {4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)
    {533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)
    {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)
    {71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)
    {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)
    {9DA2B80F-F89F-4A49-A5C2-511B085B9E8A} (Enhanced Storage Devices)
    {A0A588A4-C46F-4B37-B7EA-C82FE89870C6} (SDA Standard Compliant SD Host Controller)
    {D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)
    {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)
Thu Aug 13 22:17:26 2015 Z
    iaioi2ce.sys (Driver)
Thu Apr 21 03:11:17 2016 Z
    mcpltsvc ()
Thu Apr 21 03:13:35 2016 Z
    MCODS ()

Network  [Thu Apr 21 03:12:48 2016 Z]
Fri Jul 10 11:05:06 2015 Z
    AFD (Service)
    Ahcache.sys (Driver)
    AppInfo (Service)
    AppMgmt (Service)
    Base (Driver Group)
    BasicDisplay.sys (Driver)
    BasicRender.sys (Driver)
    BFE (Service)
    Boot Bus Extender (Driver Group)
    Boot file system (Driver Group)
    bowser (Driver)
    BrokerInfrastructure (Service)
    Browser (Service)
    CoreMessagingRegistrar (Service)
    CryptSvc (Service)
    DcomLaunch (Service)
    DeviceInstall (Service)
    dfsc (Driver)
    Dhcp (Service)
    DnsCache (Service)
    Dot3Svc (Service)
    dxgkrnl.sys (Driver)
    Eaphost (Service)
    EFS (Service)
    EventLog (Service)
    File system (Driver Group)
    Filter (Driver Group)
    FsDepends.sys (Driver)
    HelpSvc (Service)
    IKEEXT (Service)
    ipnat.sys (Driver)
    KeyIso (Service)
    LanmanServer (Service)
    LanmanWorkstation (Service)
    LmHosts (Service)
    LSM (Service)
    Messenger (Service)
    MPSDrv (Driver)
    MPSSvc (Service)
```

Page 17

SYSTEM OUTPUT.txt

```
mrxsmb (Driver)
mrxsmb10 (Driver)
mrxsmb20 (Driver)
NativeWifiP (Service)
NDIS (Driver Group)
NDIS Wrapper (Driver Group)
ndiscap (Driver)
Ndisuio (Service)
NetBIOS (Service)
NetBIOSGroup (Driver Group)
NetBT (Service)
NetDDEGroup (Driver Group)
Netlogon (Service)
NetMan (Service)
netprofm (Service)
Network (Driver Group)
NetworkProvider (Driver Group)
NlaSvc (Service)
Nsi (Service)
nsiproxy.sys (Driver)
NTDS (Service)
PCI Configuration (Driver Group)
PlugPlay (Service)
PNP Filter (Driver Group)
PNP_TDI (Driver Group)
PolicyAgent (Service)
Power (Service)
Primary disk (Driver Group)
ProfSvc (Service)
rdbss (Driver)
rdpencdd.sys (Driver)
rdsessmgr (Service)
RpcEptMapper (Service)
RpcSs (Service)
sacsvr (Service)
SCardSvr (Service)
SCSI Class (Driver Group)
sermouse.sys (Driver)
SharedAccess (Service)
SmartcardSimulator (Driver)
StateRepository (Service)
Streams Drivers (Driver Group)
SWPRV (Service)
System Bus Extender (Driver Group)
SystemEventsBroker (Service)
TabletInputService (Service)
TBS (Service)
Tcpip (Service)
TDI (Driver Group)
TileDataModelSvc (Service)
TrustedInstaller (Service)
UserManager (Service)
VaultSvc (Service)
VDS (Service)
VirtualSmartcardReader (Driver)
vmms (Service)
volmgr.sys (Driver)
volmgrx.sys (Driver)
Wcmsvc (Service)
WinDefend (Service)
WinMgmt (Service)
Wlansvc (Service)
WudfPf (Driver)
```

Page 18

SYSTEM OUTPUT.txt

```
WudfRd (Driver)
WudfSvc (Service)
WudfUsbccidDriver (Driver)
{36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)
{4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)
{4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)
{4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)
{4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)
{4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)
{4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)
{4D36E972-E325-11CE-BFC1-08002BE10318} (Net)
{4D36E973-E325-11CE-BFC1-08002BE10318} (NetClient)
{4D36E974-E325-11CE-BFC1-08002BE10318} (NetService)
{4D36E975-E325-11CE-BFC1-08002BE10318} (NetTrans)
{4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)
{4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)
{4D36E97D-E325-11CE-BFC1-08002BE10318} (System)
{4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)
{50DD5230-BA8A-11D1-BF5D-0000F805F530} (Smart card readers)
{533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)
{6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)
{71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)
{745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)
{9DA2B80F-F89F-4A49-A5C2-511B085B9E8A} (Enhanced Storage Devices)
{A0A588A4-C46F-4B37-B7EA-C82FE89870C6} (SDA Standard Compliant SD Host Controller)
{D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)
{D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)
Thu Apr 21 03:00:38 2016 Z
  McMPFSvc (Service)
Thu Apr 21 03:06:26 2016 Z
  mfemms (Service)
Thu Apr 21 03:06:57 2016 Z
  mfehidk (Service)
  mfehidk.sys (Driver)
  mfetdi2k (Service)
  mfetdi2k.sys (Driver)
  mfevtp (Service)
Thu Apr 21 03:07:02 2016 Z
  mfeaack (Service)
  mfeaack.sys (Driver)
Thu Apr 21 03:07:04 2016 Z
  mfeavfk (Service)
  mfeavfk.sys (Driver)
Thu Apr 21 03:10:33 2016 Z
  mfefirek (Service)
  mfefirek.sys (Driver)
Thu Apr 21 03:10:45 2016 Z
  mfefire (Service)
Thu Apr 21 03:11:03 2016 Z
  mcapexe ()
Thu Apr 21 03:11:17 2016 Z
  mcpltsvc ()
Thu Apr 21 03:12:48 2016 Z
  mfencbdc
  mfencbdc.sys
Thu Apr 21 03:13:35 2016 Z
  McNaiAnn ()
  MCODS ()


------------------------------------------------
services v.20080507
(System) Lists services/drivers in Services key by LastWrite times
```

Page 19

SYSTEM OUTPUT.txt

ControlSet001\Services
Lists services/drivers in Services key by LastWrite times

Thu Apr 21 04:41:25 2016Z
    Name       = mfeavfk
    Display    = McAfee Inc. mfeavfk
    ImagePath = system32\drivers\mfeavfk.sys
    Type       = Kernel driver
    Start      = Manual
    Group      =

Thu Apr 21 04:41:19 2016Z
    Name       = mfemms
    Display    = McAfee Service Controller
    ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\\mfemms.exe"
    Type       = Own_Process
    Start      = Auto Start
    Group      =

Thu Apr 21 04:41:16 2016Z
    Name       = mfeaack
    Display    = McAfee Inc. mfeaack
    ImagePath = system32\drivers\mfeaack.sys
    Type       = Kernel driver
    Start      = Manual
    Group      =

Thu Apr 21 04:41:15 2016Z
    Name       = McAfee SiteAdvisor Service
    Display    = McAfee SiteAdvisor Service
    ImagePath = "C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe"
    Type       = Own_Process
    Start      = Auto Start
    Group      =

    Name       = MCAPExe
    Display    = McAfee AP Service
    ImagePath = "C:\Program Files\McAfee\MSC\McAPExe.exe"
    Type       = Own_Process
    Start      = Auto Start
    Group      =

    Name       = McMPFSvc
    Display    = McAfee Personal Firewall Service
    ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
    Type       = Share_Process
    Start      = Auto Start
    Group      =

    Name       = McProxy
    Display    = McAfee Proxy Service
    ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
    Type       = Share_Process
    Start      = Auto Start
    Group      =

Thu Apr 21 03:24:59 2016Z
    Name       = MBAMSwissArmy
    Display    = MBAMSwissArmy
    ImagePath = \??\C:\Windows\system32\drivers\MBAMSwissArmy.sys
    Type       = File system driver
                                              Page 20

SYSTEM OUTPUT.txt

```
Start       = Manual
Group       = FSFilter Activity Monitor

Thu Apr 21 03:20:08 2016Z
  Name      = mfefirek
  Display   = McAfee Inc. mfefirek
  ImagePath = system32\drivers\mfefirek.sys
  Type      = Kernel driver
  Start     = Manual
  Group     =

Thu Apr 21 03:19:52 2016Z
  Name      = cfwids
  Display   = McAfee Inc. cfwids
  ImagePath = system32\drivers\cfwids.sys
  Type      = Kernel driver
  Start     = Manual
  Group     =

Thu Apr 21 03:19:50 2016Z
  Name      = mfencbdc
  Display   = McAfee Inc. mfencbdc
  ImagePath = \SystemRoot\system32\DRIVERS\mfencbdc.sys
  Type      = Kernel driver
  Start     = Manual
  Group     =

Thu Apr 21 03:19:31 2016Z
  Name      = UmPass
  Display   = @umpass.inf,%UmPass.SVCDESC%
  ImagePath = Microsoft UMPass Driver
  Type      = \SystemRoot\System32\drivers\umpass.sys
  Start     = Kernel driver
  Group     = Manual;Extended Base

Thu Apr 21 03:19:16 2016Z
  Name      = tunnel
  Display   = @nettun.inf,%TUNNEL.Service.DisplayName%
  ImagePath = Microsoft Tunnel Miniport Adapter Driver
  Type      = \SystemRoot\System32\drivers\tunnel.sys
  Start     = Kernel driver
  Group     = Manual;NDIS

Thu Apr 21 03:19:15 2016Z
  Name      = vwifimp
  Display   = @%SystemRoot%\System32\drivers\vwifimp.sys,-261
  ImagePath = \SystemRoot\System32\drivers\vwifimp.sys
  Type      = Kernel driver
  Start     = Manual
  Group     = NDIS

Thu Apr 21 03:18:58 2016Z
  Name      = BasicDisplay
  Display   =
  ImagePath = \SystemRoot\System32\drivers\BasicDisplay.sys
  Type      = Kernel driver
  Start     = System Start
  Group     = Video

  Name      = monitor
  Display   = @monitor.inf,%Monitor.SVCDESC%
  ImagePath = Microsoft Monitor Class Function Driver Service
  Type      = \SystemRoot\System32\drivers\monitor.sys
```

Page 21

SYSTEM OUTPUT.txt

```
    Start       = Kernel driver
    Group       = Manual;

Thu Apr 21 03:18:57 2016Z
    Name        = BtFilter
    Display     = BtFilter
    ImagePath   = \SystemRoot\system32\DRIVERS\btfilter.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

    Name        = BTHUSB
    Display     = @bth.inf,%BTHUSB.SvcDesc%
    ImagePath   = Bluetooth Radio USB Driver
    Type        = \SystemRoot\System32\Drivers\BTHUSB.sys
    Start       = Kernel driver
    Group       = Manual;PNP Filter

    Name        = RTSUER
    Display     = @oem14.inf,%RtsUER%
    ImagePath   = Realtek USB Card Reader - UER
    Type        = \SystemRoot\system32\Drivers\RtsUer.sys
    Start       = Kernel driver
    Group       = Manual;

Thu Apr 21 03:18:56 2016Z
    Name        = HidUsb
    Display     = @input.inf,%HID.SvcDesc%
    ImagePath   = Microsoft HID Class Driver
    Type        = \SystemRoot\System32\drivers\hidusb.sys
    Start       = Kernel driver
    Group       = Manual;extended base

    Name        = usbccgp
    Display     = @usb.inf,%GenericParent.SvcDesc%
    ImagePath   = Microsoft USB Generic Parent Driver
    Type        = \SystemRoot\System32\drivers\usbccgp.sys
    Start       = Kernel driver
    Group       = Manual;Base

    Name        = usbvideo
    Display     = @usbvideo.inf,%USBVideo.SvcDesc%
    ImagePath   = USB Video Device (WDM)
    Type        = \SystemRoot\System32\Drivers\usbvideo.sys
    Start       = Kernel driver
    Group       = Manual;

Thu Apr 21 03:18:55 2016Z
    Name        = ETDI2C
    Display     = @oem13.inf,%ELANI2CDeviceDesc%
    ImagePath   = ELAN I2C Filter Driver
    Type        = \SystemRoot\system32\DRIVERS\ETDI2C.sys
    Start       = Kernel driver
    Group       = Manual;Pointer Port

    Name        = hidi2c
    Display     = @hidi2c.inf,%hidi2c.SVCDESC%
    ImagePath   = Microsoft I2C HID Miniport Driver
    Type        = \SystemRoot\System32\drivers\hidi2c.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = IntcDAud
```

Page 22

```
                              SYSTEM OUTPUT.txt
   Display    = @oem6.inf,%IntcDAud.SvcDesc%
   ImagePath = Intel(R) Display Audio
   Type      = \SystemRoot\system32\DRIVERS\IntcDAud.sys
   Start     = Kernel driver
   Group     = Manual;

   Name      = mouclass
   Display   = @msmouse.inf,%mouclass.SvcDesc%
   ImagePath = Mouse Class Driver
   Type      = \SystemRoot\System32\drivers\mouclass.sys
   Start     = Kernel driver
   Group     = Manual;

   Name      = mouhid
   Display   = @msmouse.inf,%MOUHID.SvcDesc%
   ImagePath = Mouse HID Driver
   Type      = \SystemRoot\System32\drivers\mouhid.sys
   Start     = Kernel driver
   Group     = Manual;

   Name      = mshidkmdf
   Display   =
   ImagePath = \SystemRoot\System32\drivers\mshidkmdf.sys
   Type      = Kernel driver
   Start     = Manual
   Group     =

   Name      = MTConfig
   Display   = @mtconfig.inf,%MTConfig.SVCDESC%
   ImagePath = Microsoft Input Configuration Driver
   Type      = \SystemRoot\System32\drivers\MTConfig.sys
   Start     = Kernel driver
   Group     = Manual;Extended Base

Thu Apr 21 03:18:54 2016Z
   Name      = IntcAzAudAddService
   Display   = Service for Realtek HD Audio (WDM)
   ImagePath = \SystemRoot\system32\drivers\RTKVHD64.sys
   Type      = Kernel driver
   Start     = Manual
   Group     =

   Name      = ksthunk
   Display   = Kernel Streaming Thunks
   ImagePath = \SystemRoot\system32\drivers\ksthunk.sys
   Type      = Kernel driver
   Start     = Manual
   Group     = PNP Filter

   Name      = USBHUB3
   Display   = @usbhub3.inf,%UsbHub3.SVCDESC%
   ImagePath = SuperSpeed Hub
   Type      = \SystemRoot\System32\drivers\UsbHub3.sys
   Start     = Kernel driver
   Group     = Manual;Base

Thu Apr 21 03:18:51 2016Z
   Name      = mssmbios
   Display   = @mssmbios.inf,%mssmbios_svcdesc%
   ImagePath = Microsoft System Management BIOS Driver
   Type      = \SystemRoot\System32\drivers\mssmbios.sys
   Start     = Kernel driver
   Group     = System Start;
                                        Page 23
```

SYSTEM OUTPUT.txt

Thu Apr 21 03:18:49 2016Z
```
Name       = ACPI
Display    = @acpi.inf,%ACPI.SvcDesc%
ImagePath  = Microsoft ACPI Driver
Type       = System32\drivers\ACPI.sys
Start      = Kernel driver
Group      = Boot Start;Core

Name       = athr
Display    = @oem10.inf,%ATHR.Service.DispName%
ImagePath  = Qualcomm Atheros Extensible Wireless LAN device driver
Type       = \SystemRoot\System32\drivers\athw10x.sys
Start      = Kernel driver
Group      = Manual;NDIS

Name       = cdrom
Display    = @cdrom.inf,%cdrom_ServiceDesc%
ImagePath  = CD-ROM Driver
Type       = \SystemRoot\System32\drivers\cdrom.sys
Start      = Kernel driver
Group      = System Start;SCSI CDROM Class

Name       = CmBatt
Display    = @cmbatt.inf,%CmBatt.SvcDesc%
ImagePath  = Microsoft ACPI Control Method Battery Driver
Type       = \SystemRoot\System32\drivers\CmBatt.sys
Start      = Kernel driver
Group      = Manual;

Name       = disk
Display    = @disk.inf,%disk_ServiceDesc%
ImagePath  = Disk Driver
Type       = System32\drivers\disk.sys
Start      = Kernel driver
Group      = Boot Start;

Name       = EhStorClass
Display    = @%SystemRoot%\system32\drivers\EhStorClass.sys,-100
ImagePath  = System32\drivers\EhStorClass.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Class

Name       = fvevol
Display    = @%SystemRoot%\system32\drivers\fvevol.sys,-100
ImagePath  = System32\DRIVERS\fvevol.sys
Type       = Kernel driver
Start      = Boot Start
Group      = PnP Filter

Name       = GPIO
Display    = @oem4.inf,%GPIO.SVCDESC%
ImagePath  = Intel SoC GPIO Controller Driver
Type       = \SystemRoot\System32\drivers\iaiogpioe.sys
Start      = Kernel driver
Group      = Manual;

Name       = HDAudBus
Display    = @hdaudbus.inf,%HDAudBus.SVCDESC%
ImagePath  = Microsoft UAA Bus Driver for High Definition Audio
Type       = \SystemRoot\System32\drivers\HDAudBus.sys
Start      = Kernel driver
```

Page 24

```
                              SYSTEM OUTPUT.txt
Group       = Manual;Extended Base

Name        = i8042prt
Display     = @keyboard.inf,%i8042prt.SvcDesc%
ImagePath   = i8042 Keyboard and PS/2 Mouse Port Driver
Type        = \SystemRoot\System32\drivers\i8042prt.sys
Start       = Kernel driver
Group       = Manual;Keyboard Port

Name        = iaioi2c
Display     = @oem5.inf,%Driver_Service.Desc%
ImagePath   = I2C Controller Service
Type        = \SystemRoot\System32\drivers\iaioi2ce.sys
Start       = Kernel driver
Group       = Manual;

Name        = igfx
Display     =
ImagePath   = \SystemRoot\system32\DRIVERS\igdkmd64.sys
Type        = Kernel driver
Start       = Manual
Group       = Video

Name        = intelpep
Display     = @intelpep.inf,%INTELPEP.SVCDESC%
ImagePath   = Intel(R) Power Engine Plug-in Driver
Type        = System32\drivers\intelpep.sys
Start       = Kernel driver
Group       = Boot Start;

Name        = intelppm
Display     = @cpu.inf,%IntelPPM.SvcDesc%
ImagePath   = Intel Processor Driver
Type        = \SystemRoot\System32\drivers\intelppm.sys
Start       = Kernel driver
Group       = Manual;Extended Base

Name        = kbdclass
Display     = @keyboard.inf,%kbdclass.SvcDesc%
ImagePath   = Keyboard Class Driver
Type        = \SystemRoot\System32\drivers\kbdclass.sys
Start       = Kernel driver
Group       = Manual;

Name        = mfewfpk
Display     = McAfee Inc. mfewfpk
ImagePath   = system32\drivers\mfewfpk.sys
Type        = Kernel driver
Start       = Boot Start
Group       = NDIS

Name        = msisadrv
Display     =
ImagePath   = System32\drivers\msisadrv.sys
Type        = Kernel driver
Start       = Boot Start
Group       = Boot Bus Extender

Name        = partmgr
Display     = @%SystemRoot%\system32\drivers\partmgr.sys,-100
ImagePath   = System32\drivers\partmgr.sys
Type        = Kernel driver
Start       = Boot Start
```

Page 25

```
                              SYSTEM OUTPUT.txt
Group       = Boot Bus Extender

Name        = pci
Display     = @pci.inf,%pci_svcdesc%
ImagePath   = PCI Bus Driver
Type        = System32\drivers\pci.sys
Start       = Kernel driver
Group       = Boot Start;Boot Bus Extender

Name        = rdyboost
Display     = ReadyBoost
ImagePath   = System32\drivers\rdyboost.sys
Type        = Kernel driver
Start       = Boot Start
Group       = PnP Filter

Name        = rt640x64
Display     = @oem12.inf,%rt640.Service.DispName%
ImagePath   = Realtek RT640 NT Driver
Type        = \SystemRoot\System32\drivers\rt640x64.sys
Start       = Kernel driver
Group       = Manual;NDIS

Name        = storahci
Display     = @mshdc.inf,%storahci_ServiceDescription%
ImagePath   = Microsoft Standard SATA AHCI Driver
Type        = System32\drivers\storahci.sys
Start       = Kernel driver
Group       = Boot Start;SCSI Miniport

Name        = TXEIx64
Display     = @oem2.inf,%TEE_SvcDesc%
ImagePath   = Intel(R) Trusted Execution Engine Interface
Type        = \SystemRoot\System32\drivers\TXEIx64.sys
Start       = Kernel driver
Group       = Manual;Extended Base

Name        = UEFI
Display     = @uefi.inf,%UEFI.SvcDesc%
ImagePath   = Microsoft UEFI Driver
Type        = \SystemRoot\System32\drivers\UEFI.sys
Start       = Kernel driver
Group       = Manual;

Name        = USBXHCI
Display     = @usbxhci.inf,%PCI\CC_0C0330.DeviceDesc%
ImagePath   = USB xHCI Compliant Host Controller
Type        = \SystemRoot\System32\drivers\USBXHCI.SYS
Start       = Kernel driver
Group       = Manual;

Name        = volsnap
Display     = @volume.inf,%VolumeClassName%
ImagePath   = Storage volumes
Type        = System32\drivers\volsnap.sys
Start       = Kernel driver
Group       = Boot Start;

Name        = vwifibus
Display     = @%SystemRoot%\System32\drivers\vwifibus.sys,-257
ImagePath   = \SystemRoot\System32\drivers\vwifibus.sys
Type        = Kernel driver
Start       = Manual
                                 Page 26
```

SYSTEM OUTPUT.txt

```
Group       =

Name        = Wdf01000
Display     = @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000
ImagePath   = system32\drivers\Wdf01000.sys
Type        = Kernel driver
Start       = Boot Start
Group       = WdfLoadGroup

Name        = WmiAcpi
Display     = @wmiacpi.inf,%WMIMAP.SvcDesc%
ImagePath   = Microsoft Windows Management Interface for ACPI
Type        = \SystemRoot\System32\drivers\wmiacpi.sys
Start       = Kernel driver
Group       = Manual;Extended Base

Thu Apr 21 03:18:48 2016Z
Name        = BasicRender
Display     =
ImagePath   = \SystemRoot\System32\drivers\BasicRender.sys
Type        = Kernel driver
Start       = System Start
Group       = Video

Name        = CompositeBus
Display     = @compositebus.inf,%CompositeBus.SVCDESC%
ImagePath   = Composite Bus Enumerator Driver
Type        =
\SystemRoot\System32\DriverStore\FileRepository\compositebus.inf_amd64_98334ba6e7685
3ba\CompositeBus.sys
Start       = Kernel driver
Group       = Manual;Extended Base

Name        = iwdbus
Display     = @oem9.inf,%iwdbus.SVCDESC%
ImagePath   = IWD Bus Enumerator
Type        = \SystemRoot\System32\drivers\iwdbus.sys
Start       = Kernel driver
Group       = Manual;Extended Base

Name        = kdnic
Display     = @kdnic.inf,%KdNic.Service.DispName%
ImagePath   = Microsoft Kernel Debug Network Miniport (NDIS 6.20)
Type        = \SystemRoot\System32\drivers\kdnic.sys
Start       = Kernel driver
Group       = Manual;NDIS

Name        = LMDriver
Display     = @oem16.inf,%LMDriver.SVCDESC%
ImagePath   = Launch Manager Wireless Driver
Type        = \SystemRoot\System32\drivers\LMDriver.sys
Start       = Kernel driver
Group       = Manual;

Name        = NdisVirtualBus
Display     = @%SystemRoot%\System32\drivers\NdisVirtualBus.sys,-200
ImagePath   = \SystemRoot\System32\drivers\NdisVirtualBus.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = RadioShim
Display     = @oem16.inf,%RadioShim.SVCDESC%
```

Page 27

SYSTEM OUTPUT.txt
```
    ImagePath = Shim for HID-KMDF Interface layer
    Type      = \SystemRoot\System32\drivers\RadioShim.sys
    Start     = Kernel driver
    Group     = Manual;PNP Filter

    Name      = rdpbus
    Display   = @rdpbus.inf,%rdpbus_svcdesc%
    ImagePath = Remote Desktop Device Redirector Bus Driver
    Type      = \SystemRoot\System32\drivers\rdpbus.sys
    Start     = Kernel driver
    Group     = Manual;

    Name      = spaceport
    Display   = @spaceport.inf,%Spaceport_ServiceDesc%
    ImagePath = Storage Spaces Driver
    Type      = System32\drivers\spaceport.sys
    Start     = Kernel driver
    Group     = Boot Start;System Bus Extender

    Name      = swenum
    Display   = @swenum.inf,%SWENUM.SVCDESC%
    ImagePath = Software Bus Driver
    Type      =
\SystemRoot\System32\DriverStore\FileRepository\swenum.inf_amd64_2a699e44676b7781\sw
enum.sys
    Start     = Kernel driver
    Group     = Manual;Extended Base

    Name      = tap0901
    Display   = @oem23.inf,%DeviceDescription%
    ImagePath = TAP-Windows Adapter V9
    Type      = \SystemRoot\System32\drivers\tap0901.sys
    Start     = Kernel driver
    Group     = Manual;NDIS

    Name      = umbus
    Display   = @umbus.inf,%umbus.SVCDESC%
    ImagePath = UMBus Enumerator Driver
    Type      = \SystemRoot\System32\drivers\umbus.sys
    Start     = Kernel driver
    Group     = Manual;Extended Base

    Name      = vdrvroot
    Display   = @vdrvroot.inf,%vdrvroot_svcdesc%
    ImagePath = Microsoft Virtual Drive Enumerator
    Type      = System32\drivers\vdrvroot.sys
    Start     = Kernel driver
    Group     = Boot Start;Boot Bus Extender

    Name      = volmgr
    Display   = @volmgr.inf,%volmgr_svcdesc%
    ImagePath = Volume Manager Driver
    Type      = System32\drivers\volmgr.sys
    Start     = Kernel driver
    Group     = Boot Start;System Bus Extender

Thu Apr 21 03:15:49 2016Z
    Name      = mfesapsn
    Display   = McAfee Process Start Notification Service
    ImagePath = \??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =
```
Page 28

SYSTEM OUTPUT.txt

```
Thu Apr 21 03:15:18 2016Z
    Name       = McPvDrv
    Display    = McPvDrv Driver
    ImagePath  = \SystemRoot\system32\drivers\McPvDrv.sys
    Type       = Kernel driver
    Start      = Auto Start
    Group      =

Thu Apr 21 03:15:06 2016Z
    Name       = MSK80Service
    Display    = McAfee Anti-Spam Service
    ImagePath  = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
    Type       = Share_Process
    Start      = Auto Start
    Group      =

Thu Apr 21 03:14:14 2016Z
    Name       = HipShieldK
    Display    = McAfee Inc. HipShieldK
    ImagePath  = system32\drivers\HipShieldK.sys
    Type       = Kernel driver
    Start      = Manual
    Group      =

Thu Apr 21 03:13:53 2016Z
    Name       = WdBoot
    Display    = @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-390
    ImagePath  = \SystemRoot\system32\drivers\WdBoot.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = _Early-Launch

    Name       = WdFilter
    Display    = @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-330
    ImagePath  = \SystemRoot\system32\drivers\WdFilter.sys
    Type       = File system driver
    Start      = Manual
    Group      = FSFilter Anti-Virus

Thu Apr 21 03:13:47 2016Z
    Name       = mfehidk
    Display    = McAfee Inc. mfehidk
    ImagePath  = system32\drivers\mfehidk.sys
    Type       = Kernel driver
    Start      = Boot Start
    Group      = FSFilter Anti-Virus

    Name       = WinDefend
    Display    = @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310
    ImagePath  = "%ProgramFiles%\Windows Defender\MsMpEng.exe"
    Type       = Own_Process
    Start      = Manual
    Group      =

Thu Apr 21 03:13:46 2016Z
    Name       = WdNisDrv
    Display    = @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-370
    ImagePath  = system32\Drivers\WdNisDrv.sys
    Type       = Kernel driver
    Start      = Manual
    Group      =
```

Page 29

SYSTEM OUTPUT.txt

```
Thu Apr 21 03:13:35 2016Z
   Name        = MCODS
   Display     = McAfee Scanner
   ImagePath = "C:\Program Files\McAfee\VirusScan\mcods.exe"
   Type        = Own_Process
   Start       = Manual
   Group       =

Thu Apr 21 03:13:25 2016Z
   Name        = McNaiAnn
   Display     = McAfee VirusScan Announcer
   ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
   Type        = Share_Process
   Start       = Auto Start
   Group       =

Thu Apr 21 03:12:49 2016Z
   Name        = mfencrk
   Display     = McAfee Inc. mfencrk
   ImagePath = \SystemRoot\system32\DRIVERS\mfencrk.sys
   Type        = Kernel driver
   Start       = Manual
   Group       =

Thu Apr 21 03:12:03 2016Z
   Name        = McBootDelayStartSvc
   Display     = McAfee Boot Delay Start Service
   ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
   Type        = Share_Process
   Start       = Auto Start
   Group       =

Thu Apr 21 03:12:02 2016Z
   Name        = mcpltsvc
   Display     = McAfee Platform Services
   ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
   Type        = Share_Process
   Start       = Auto Start
   Group       =

Thu Apr 21 03:11:46 2016Z
   Name        = PEFService
   Display     = Intel Security PEF Service
   ImagePath = "C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFService.exe"
   Type        = Own_Process
   Start       = Auto Start
   Group       =

Thu Apr 21 03:11:37 2016Z
   Name        = mccspsvc
   Display     = McAfee CSP Service
   ImagePath = "C:\Program Files\Common
Files\McAfee\CSP\1.9.656.0\McCSPServiceHost.exe"
   Type        = Own_Process
   Start       = Auto Start
   Group       =

Thu Apr 21 03:10:59 2016Z
   Name        = HomeNetSvc
```

Page 30

SYSTEM OUTPUT.txt
```
    Display    = McAfee Home Network
    ImagePath  = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc
    Type       = Share_Process
    Start      = Auto Start
    Group      =

Thu Apr 21 03:10:58 2016Z
    Name       = mfefire
    Display    = McAfee Firewall Core Service
    ImagePath  = "C:\Program Files\Common Files\McAfee\SystemCore\\mfefire.exe"
    Type       = Own_Process
    Start      = Manual
    Group      =

Thu Apr 21 03:10:57 2016Z
    Name       = mfevtp
    Display    = McAfee Validation Trust Protection Service
    ImagePath  = "C:\Windows\system32\mfevtps.exe"
    Type       = Own_Process
    Start      = Manual
    Group      =

Thu Apr 21 03:10:48 2016Z
    Name       = mfeelamk
    Display    = McAfee Inc. mfeelamk
    ImagePath  = system32\drivers\mfeelamk.sys
    Type       = Kernel driver
    Start      = Boot Start
    Group      = Early-Launch

Thu Apr 21 03:08:54 2016Z
    Name       = ModuleCoreService
    Display    = McAfee Module Core Service
    ImagePath  = "C:\Program Files\Common
Files\McAfee\ModuleCore\ModuleCoreService.exe"
    Type       = Share_Process
    Start      = Auto Start
    Group      =

Thu Apr 21 03:00:51 2016Z
    Name       = BITS
    Display    = @%SystemRoot%\system32\qmgr.dll,-1000
    ImagePath  = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type       = Share_Process
    Start      = Auto Start
    Group      =

Sun Apr 17 00:48:02 2016Z
    Name       = TrustedInstaller
    Display    = @%SystemRoot%\servicing\TrustedInstaller.exe,-100
    ImagePath  = %SystemRoot%\servicing\TrustedInstaller.exe
    Type       = Own_Process
    Start      = Manual
    Group      = ProfSvc_Group

Sun Apr 17 00:44:02 2016Z
    Name       = BthLEEnum
    Display    = @bthleenum.inf,%BthLEEnum.SVCDESC%
    ImagePath  = Bluetooth Low Energy Driver
    Type       = \SystemRoot\System32\drivers\BthLEEnum.sys
    Start      = Kernel driver
    Group      = Manual;
```
Page 31

SYSTEM OUTPUT.txt

```
Name       = Parport
Display    = @msports.inf,%Parport.SVCDESC%
ImagePath  = Parallel port driver
Type       = \SystemRoot\System32\drivers\parport.sys
Start      = Kernel driver
Group      = Manual;Parallel arbitrator

Name       = Serenum
Display    = @msports.inf,%Serenum.SVCDESC%
ImagePath  = Serenum Filter Driver
Type       = \SystemRoot\System32\drivers\serenum.sys
Start      = Kernel driver
Group      = Manual;PNP Filter

Name       = Serial
Display    = @msports.inf,%Serial.SVCDESC%
ImagePath  = Serial port driver
Type       = \SystemRoot\System32\drivers\serial.sys
Start      = Kernel driver
Group      = Manual;Extended base

Name       = usbser
Display    = @usbser.inf,%UsbSerial.DriverDesc%
ImagePath  = Microsoft USB Serial Driver
Type       = \SystemRoot\System32\drivers\usbser.sys
Start      = Kernel driver
Group      = Manual;

Name       = USBSTOR
Display    = @usbstor.inf,%USBSTOR.SvcDesc%
ImagePath  = USB Mass Storage Driver
Type       = \SystemRoot\System32\drivers\USBSTOR.SYS
Start      = Kernel driver
Group      = Manual;

Tue Apr 12 20:56:49 2016Z
Name       = YahooAUService
Display    = Yahoo! Updater
ImagePath  = "C:\Program Files (x86)\Yahoo!\SoftwareUpdate\YahooAUService.exe"
Type       = Own_Process
Start      = Auto Start
Group      =

Tue Apr  5 22:21:01 2016Z
Name       = MSPCLOCK
Display    = @ksfilter.inf,%MSPCLOCK.DeviceDesc%
ImagePath  = Microsoft Streaming Clock Proxy
Type       = \SystemRoot\system32\drivers\MSPCLOCK.sys
Start      = Kernel driver
Group      = Manual;Extended Base

Tue Apr  5 22:21:00 2016Z
Name       = MSPQM
Display    = @ksfilter.inf,%MSPQM.DeviceDesc%
ImagePath  = Microsoft Streaming Quality Manager Proxy
Type       = \SystemRoot\system32\drivers\MSPQM.sys
Start      = Kernel driver
Group      = Manual;Extended Base

Sat Apr  2 16:10:08 2016Z
Name       = BthAvrcpTg
Display    = @bthaudhid.inf,%BthAvrcpTg_SvcDesc%
```

Page 32

```
                              SYSTEM OUTPUT.txt
    ImagePath = Bluetooth Audio/Video Remote Control HID
    Type      = \SystemRoot\System32\drivers\BthAvrcpTg.sys
    Start     = Kernel driver
    Group     = Manual;Extended Base

Sat Apr  2 16:08:56 2016Z
    Name      = BthPan
    Display   = @bthpan.inf,%BthPan.DisplayName%
    ImagePath = Bluetooth Device (Personal Area Network)
    Type      = \SystemRoot\System32\drivers\bthpan.sys
    Start     = Kernel driver
    Group     = Manual;NDIS

Sat Apr  2 16:08:55 2016Z
    Name      = BthEnum
    Display   = @bth.inf,%BthEnum.SVCDESC%
    ImagePath = Bluetooth Enumerator Service
    Type      = \SystemRoot\System32\drivers\BthEnum.sys
    Start     = Kernel driver
    Group     = Manual;

    Name      = RFCOMM
    Display   = @tdibth.inf,%RFCOMM.DisplayName%
    ImagePath = Bluetooth Device (RFCOMM Protocol TDI)
    Type      = \SystemRoot\System32\drivers\rfcomm.sys
    Start     = Kernel driver
    Group     = Manual;PNP_TDI

Tue Mar 29 09:31:18 2016Z
    Name      = NdisTapi
    Display   = @%systemroot%\system32\rascfg.dll,-32001
    ImagePath = System32\DRIVERS\ndistapi.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = NDIS

    Name      = NdisWan
    Display   = @%systemroot%\system32\rascfg.dll,-32002
    ImagePath = \SystemRoot\System32\drivers\ndiswan.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = PptpMiniport
    Display   = @%systemroot%\system32\rascfg.dll,-32006
    ImagePath = \SystemRoot\System32\drivers\raspptp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = Rasl2tp
    Display   = @%systemroot%\system32\rascfg.dll,-32005
    ImagePath = \SystemRoot\System32\drivers\rasl2tp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = RasPppoe
    Display   = @%systemroot%\system32\rascfg.dll,-32007
    ImagePath = \SystemRoot\System32\drivers\raspppoe.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =
```

Page 33

SYSTEM OUTPUT.txt

```
Tue Mar 29 09:31:17 2016Z
    Name      = RasAgileVpn
    Display   = @netavpna.inf,%Svc-Mp-AgileVpn-DispName%
    ImagePath = WAN Miniport (IKEv2)
    Type      = \SystemRoot\System32\drivers\AgileVpn.sys
    Start     = Kernel driver
    Group     = Manual;

Tue Mar 29 09:31:16 2016Z
    Name      = RasSstp
    Display   = @%systemroot%\system32\sstpsvc.dll,-202
    ImagePath = \SystemRoot\System32\drivers\rassstp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

Tue Mar 29 09:29:40 2016Z
    Name      = DeviceAssociationService
    Display   = @%SystemRoot%\system32\das.dll,-100
    ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
    Type      = Share_Process
    Start     = Auto Start
    Group     =

Tue Mar 29 09:22:07 2016Z
    Name      = lltdio
    Display   = @%SystemRoot%\system32\lltdres.dll,-6
    ImagePath = system32\drivers\lltdio.sys
    Type      = Kernel driver
    Start     = Auto Start
    Group     = NDIS

    Name      = ndiswanlegacy
    Display   = @%systemroot%\system32\rascfg.dll,-32014
    ImagePath = System32\DRIVERS\ndiswan.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = NDIS

    Name      = rspndr
    Display   = @%SystemRoot%\system32\lltdres.dll,-5
    ImagePath = system32\drivers\rspndr.sys
    Type      = Kernel driver
    Start     = Auto Start
    Group     = NDIS

    Name      = wanarp
    Display   = @%systemroot%\system32\rascfg.dll,-32011
    ImagePath = System32\DRIVERS\wanarp.sys
    Type      = Kernel driver
    Start     = Auto Start
    Group     = NDIS

    Name      = wanarpv6
    Display   = @%systemroot%\system32\rascfg.dll,-32012
    ImagePath = System32\DRIVERS\wanarp.sys
    Type      = Kernel driver
    Start     = Manual
    Group     = NDIS

Sun Mar 27 13:05:49 2016Z
    Name      = ESProtectionDriver
```

Page 34

```
                          SYSTEM OUTPUT.txt
Display    = Malwarebytes Anti-Exploit
ImagePath  = \??\C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae64.sys
Type       = Kernel driver
Start      = System Start
Group      =

Name       = MbaeSvc
Display    = Malwarebytes Anti-Exploit Service
ImagePath  = "C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae-svc.exe"
Type       = Own_Process
Start      = Auto Start
Group      =

Wed Mar 23 10:11:59 2016Z
Name       = OpenVPNService
Display    = OpenVPN Service
ImagePath  = "C:\Program Files (x86)\HMA! Pro VPN\bin\openvpnserv.exe"
Type       = Own_Process
Start      = Manual
Group      =

Wed Mar 23 10:11:15 2016Z
Name       = ndproxy
Display    = @%SystemRoot%\system32\drivers\todo.sys,-101
ImagePath  = NDIS Proxy
Type       = System32\DRIVERS\NDProxy.sys
Start      = Kernel driver
Group      = Manual;PNP_TDI

Wed Mar 23 09:50:47 2016Z
Name       = BrSerIb
Display    = @oem20.inf,%BrSerIb.SvcDesc%
ImagePath  = Brother Serial Interface Driver(WDM)
Type       = \SystemRoot\system32\DRIVERS\BrSerIb.sys
Start      = Kernel driver
Group      = Manual;

Name       = BrUsbSIb
Display    = @oem20.inf,%BrUsbSIb.SvcDesc%
ImagePath  = Brother Serial USB Driver(WDM)
Type       = \SystemRoot\system32\DRIVERS\BrUsbSIb.sys
Start      = Kernel driver
Group      = Manual;

Name       = usbprint
Display    = @usbprint.inf,%USBPRINT.SvcDesc%
ImagePath  = Microsoft USB PRINTER Class
Type       = \SystemRoot\System32\drivers\usbprint.sys
Start      = Kernel driver
Group      = Manual;extended base

Name       = usbscan
Display    = @sti.inf,%usbscan.SvcDesc%
ImagePath  = USB Scanner Driver
Type       = \SystemRoot\system32\DRIVERS\usbscan.sys
Start      = Kernel driver
Group      = Manual;Base

Wed Mar 23 09:50:26 2016Z
Name       = stornvme
Display    = @stornvme.inf,%StorNVMe_ServiceDesc%
ImagePath  = Microsoft Standard NVM Express Driver
Type       = System32\drivers\stornvme.sys
                          Page 35
```

SYSTEM OUTPUT.txt
```
Start       = Kernel driver
Group       = Boot Start;SCSI Miniport

Wed Mar 23 09:48:50 2016Z
    Name        = BthHFEnum
    Display     = @bthhfenum.inf,%BthHFEnum.SVCDESC%
    ImagePath   = Bluetooth Hands-Free Audio and Call Control HID Enumerator
    Type        = \SystemRoot\System32\drivers\bthhfenum.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = BthHFSrv
    Display     = @%SystemRoot%\System32\BthHFSrv.dll,-103
    ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceAndNoImpersonation
    Type        = Share_Process
    Start       = Manual
    Group       =

    Name        = BTHPORT
    Display     = @bth.inf,%BTHPORT.SvcDesc%
    ImagePath   = Bluetooth Port Driver
    Type        = \SystemRoot\System32\Drivers\BTHport.sys
    Start       = Kernel driver
    Group       = Manual;PNP Filter

    Name        = buttonconverter
    Display     = @buttonconverter.inf,%btnconv.SvcDesc%
    ImagePath   = Service for Portable Device Control devices
    Type        = \SystemRoot\System32\drivers\buttonconverter.sys
    Start       = Kernel driver
    Group       = Manual;

    Name        = drmkaud
    Display     = @wdmaudio.inf,%drmkaud.SvcDesc%
    ImagePath   = Microsoft Trusted Audio Drivers
    Type        = \SystemRoot\system32\drivers\drmkaud.sys
    Start       = Kernel driver
    Group       = Manual;

    Name        = msgpiowin32
    Display     = @msgpiowin32.inf,%GPIO.SvcDesc%
    ImagePath   = Common Driver for Buttons, DockMode and Laptop/Slate Indicator
    Type        = \SystemRoot\System32\drivers\msgpiowin32.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = sdbus
    Display     =
    ImagePath   = \SystemRoot\System32\drivers\sdbus.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = System Bus Extender

    Name        = usbehci
    Display     = @usbport.inf,%EHCIMP.SvcDesc%
    ImagePath   = Microsoft USB 2.0 Enhanced Host Controller Miniport Driver
    Type        = \SystemRoot\System32\drivers\usbehci.sys
    Start       = Kernel driver
    Group       = Manual;Base

    Name        = usbhub
    Display     = @usbport.inf,%ROOTHUB.SvcDesc%
    ImagePath   = Microsoft USB Standard Hub Driver
```
Page 36

```
                              SYSTEM OUTPUT.txt
    Type        = \SystemRoot\System32\drivers\usbhub.sys
    Start       = Kernel driver
    Group       = Manual;Base

    Name        = usbohci
    Display     = @usbport.inf,%OHCIMP.SvcDesc%
    ImagePath   = Microsoft USB Open Host Controller Miniport Driver
    Type        = \SystemRoot\System32\drivers\usbohci.sys
    Start       = Kernel driver
    Group       = Manual;Base

    Name        = usbuhci
    Display     = @usbport.inf,%UHCIMP.SvcDesc%
    ImagePath   = Microsoft USB Universal Host Controller Miniport Driver
    Type        = \SystemRoot\System32\drivers\usbuhci.sys
    Start       = Kernel driver
    Group       = Manual;Base

Wed Mar 23 09:41:44 2016Z
    Name        = BrYNSvc
    Display     = BrYNSvc
    ImagePath   = "C:\Program Files (x86)\Browny02\BrYNSvc.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

Wed Mar 23 09:25:17 2016Z
    Name        = stisvc
    Display     = @%SystemRoot%\system32\wiaservc.dll,-9
    ImagePath   = %SystemRoot%\system32\svchost.exe -k imgsvc
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Tue Mar 22 13:52:39 2016Z
    Name        = MsBridge
    Display     = @%SystemRoot%\system32\bridgeres.dll,-1
    ImagePath   = System32\drivers\bridge.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = NDIS

Tue Mar 22 13:52:38 2016Z
    Name        = Ndisuio
    Display     = NDIS Usermode I/O Protocol
    ImagePath   = system32\drivers\ndisuio.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = NDIS

    Name        = xboxgip
    Display     = @xboxgip.inf,%XBOXGIP_Desc%
    ImagePath   = Xbox Game Input Protocol Driver
    Type        = \SystemRoot\System32\drivers\xboxgip.sys
    Start       = Kernel driver
    Group       = Manual;NDIS

Tue Mar 22 13:31:01 2016Z
    Name        = CCDMonitorService
    Display     = CCDMonitorService
    ImagePath   = C:\Program Files (x86)\Acer\AOP Framework\CCDMonitorService.exe
    Type        = Own_Process
    Start       = Auto Start
```

Page 37

SYSTEM OUTPUT.txt

```
    Group       =

Tue Mar 22 13:31:00 2016z
    Name        = ose
    Display     = Office Source Engine
    ImagePath = "C:\Program Files (x86)\Common Files\Microsoft Shared\Source
Engine\OSE.EXE"
    Type        = Own_Process
    Start       = Manual
    Group       =

Tue Mar 22 13:18:45 2016z
    Name        = IKEEXT
    Display     = @%SystemRoot%\system32\ikeext.dll,-501
    ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

Tue Mar 22 13:16:27 2016z
    Name        = MSDTC Bridge 3.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = MSDTC Bridge 4.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = ServiceModelEndpoint 3.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = ServiceModelOperation 3.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = ServiceModelService 3.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = SMSvcHost 3.0.0.0
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = SMSvcHost 4.0.0.0
```

Page 38

SYSTEM OUTPUT.txt

```
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = Windows Workflow Foundation 3.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = Windows Workflow Foundation 4.0.0.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Tue Mar 22 13:15:54 2016Z
    Name       = intaud_WaveExtensible
    Display    = @oem8.inf,%INTAUD_WEX.SvcDesc%
    ImagePath  = Intel WiDi Audio Device
    Type       = \SystemRoot\system32\drivers\intelaud.sys
    Start      = Kernel driver
    Group      = Manual;

Tue Mar 22 13:15:48 2016Z
    Name       = MSKSSRV
    Display    = @ksfilter.inf,%MSKSSRV.DeviceDesc%
    ImagePath  = Microsoft Streaming Service Proxy
    Type       = \SystemRoot\system32\drivers\MSKSSRV.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = MSTEE
    Display    = @ksfilter.inf,%MSTEE.DeviceDesc%
    ImagePath  = Microsoft Streaming Tee/Sink-to-Sink Converter
    Type       = \SystemRoot\system32\drivers\MSTEE.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

Tue Mar 22 13:15:31 2016Z
    Name       = igfxCUIService1.0.0.0
    Display    = Intel(R) HD Graphics Control Panel Service
    ImagePath  = %SystemRoot%\system32\igfxCUIService.exe
    Type       = Own_Process
    Start      = Auto Start
    Group      = ProfSvc_Group

Tue Mar 22 12:21:54 2016Z
    Name       = EventLog
    Display    = @%SystemRoot%\system32\wevtsvc.dll,-200
    ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
    Type       = Share_Process
    Start      = Auto Start
    Group      = Event Log

Tue Mar 22 11:54:41 2016Z
    Name       = MBAMScheduler
    Display    =
    ImagePath  = "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe"
```

Page 39

SYSTEM OUTPUT.txt
```
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Tue Mar 22 11:54:39 2016Z
    Name        = MBAMService
    Display     =
    ImagePath   = "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe"
    Type        = Own_Process
    Start       = Auto Start
    Group       =

    Name        = MBAMWebAccessControl
    Display     =
    ImagePath   = \??\C:\Windows\system32\drivers\mwac.sys
    Type        = File system driver
    Start       = Manual
    Group       =

Tue Mar 22 11:54:38 2016Z
    Name        = MBAMProtector
    Display     =
    ImagePath   = \??\C:\Windows\system32\drivers\mbam.sys
    Type        = File system driver
    Start       = Manual
    Group       = FSFilter Anti-Virus

Tue Mar 22 11:21:46 2016Z
    Name        = cphs
    Display     = Intel(R) Content Protection HECI Service
    ImagePath   = %SystemRoot%\SysWow64\IntelCpHeciSvc.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

Tue Mar 22 10:37:21 2016Z
    Name        = odserv
    Display     = Microsoft Office Diagnostics Service
    ImagePath   = "C:\Program Files (x86)\Common Files\Microsoft
Shared\OFFICE12\ODSERV.EXE"
    Type        = Own_Process
    Start       = Manual
    Group       =

Fri Sep 11 09:45:22 2015Z
    Name        = WpdUpFltr
    Display     = @%systemroot%\System32\drivers\WpdUpFltr.sys,-100
    ImagePath   = System32\drivers\WpdUpFltr.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = PnP Filter

    Name        = WUDFWpdFs
    Display     =
    ImagePath   = \SystemRoot\system32\DRIVERS\WUDFRd.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

Thu Aug 13 23:24:15 2015Z
    Name        = WSearch
    Display     = @%systemroot%\system32\SearchIndexer.exe,-103
    ImagePath   = %systemroot%\system32\SearchIndexer.exe /Embedding
```
Page 40

SYSTEM OUTPUT.txt

```
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Thu Aug 13 23:03:20 2015z
    Name        = MSDTC
    Display     = @comres.dll,-2797
    ImagePath   = %SystemRoot%\System32\msdtc.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Aug 13 22:52:11 2015z
    Name        = UcmUcsi
    Display     = @ucmucsi.inf,%UcmUcsi.ServiceName%
    ImagePath   = USB Connector Manager UCSI Client
    Type        = \SystemRoot\System32\drivers\UcmUcsi.sys
    Start       = Kernel driver
    Group       = Manual;

Thu Aug 13 22:37:27 2015z
    Name        = ePowerSvc
    Display     = ePower Service
    ImagePath   = "C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Aug 13 22:35:41 2015z
    Name        = QALSvc
    Display     = Quick Access Local Service
    ImagePath   = "C:\Program Files\Acer\Acer Quick Access\QALSvc.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

    Name        = QASvc
    Display     = Quick Access Service
    ImagePath   = "C:\Program Files\Acer\Acer Quick Access\QASvc.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Aug 13 22:34:01 2015z
    Name        = Dashlane Upgrade Service
    Display     =
    ImagePath   = "C:\Program Files (x86)\Dashlane\Upgrade\DashlaneUpgradeService.exe"
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Thu Aug 13 22:33:48 2015z
    Name        = Amazon 1Button App Service
    Display     = Amazon 1Button App Service
    ImagePath   = "c:\Program Files
(x86)\Amazon\Amazon1ButtonApp\Amazon1ButtonService64.Exe"
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Thu Aug 13 22:25:21 2015z
    Name        = AtherosSvc
    Display     = AtherosSvc
```

Page 41

```
                              SYSTEM OUTPUT.txt
   ImagePath = "C:\Program Files (x86)\Qualcomm Atheros\Bluetooth
Suite\adminservice.exe"
   Type        = Own_Process
   Start       = Auto Start
   Group       =

Thu Aug 13 22:19:13 2015z
   Name        = ICCS
   Display     = Intel(R) Integrated Clock Controller Service - Intel(R) ICCS
   ImagePath = "C:\Program Files (x86)\Intel\Intel(R) Integrated Clock Controller
Service\ICCProxy.exe"
   Type        = Own_Process
   Start       = Manual
   Group       =

Thu Aug 13 22:19:11 2015z
   Name        = ialm
   Display     =
   ImagePath =
   Type        =
   Start       =
   Group       =

Thu Aug 13 22:15:02 2015z
   Name        = Intel(R) Capability Licensing Service TCP IP Interface
   Display     = Intel(R) Capability Licensing Service TCP IP Interface
   ImagePath = "C:\Program Files\Intel\TXE Components\TCS\SocketHeciServer.exe"
   Type        = Own_Process
   Start       = Manual
   Group       =

Thu Aug 13 22:13:17 2015z
   Name        = HdAudAddService
   Display     = @hdaudio.inf,%UAAFunctionDriverForHdAudio.SvcDesc%
   ImagePath = Microsoft 1.1 UAA Function Driver for High Definition Audio Service
   Type        = \SystemRoot\system32\DRIVERS\HdAudio.sys
   Start       = Kernel driver
   Group       = Manual;

Thu Aug 13 21:56:11 2015z
   Name        = WlanSvc
   Display     = @%SystemRoot%\System32\wlansvc.dll,-257
   ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
   Type        = Share_Process
   Start       = Auto Start
   Group       = TDI

Thu Aug 13 21:55:42 2015z
   Name        = acpipagr
   Display     = @acpipagr.inf,%SvcDesc%
   ImagePath = ACPI Processor Aggregator Driver
   Type        = \SystemRoot\System32\drivers\acpipagr.sys
   Start       = Kernel driver
   Group       = Manual;

   Name        = iaLPSSi_GPIO
   Display     = @ialpssi_gpio.inf,%iaLPSSi_GPIO.SVCDESC%
   ImagePath = Intel(R) Serial IO GPIO Controller Driver
   Type        = \SystemRoot\System32\drivers\iaLPSSi_GPIO.sys
   Start       = Kernel driver
   Group       = Manual;Extended Base

   Name        = iaLPSSi_I2C
```

Page 42

```
                              SYSTEM OUTPUT.txt
Display    = @ialpssi_i2c.inf,%iaLPSSi_I2C.SVCDESC%
ImagePath  = Intel(R) Serial IO I2C Controller Driver
Type       = \SystemRoot\System32\drivers\iaLPSSi_I2C.sys
Start      = Kernel driver
Group      = Manual;Base

Name       = TPM
Display    = @tpm.inf,%TPM%
ImagePath  = TPM
Type       = \SystemRoot\system32\drivers\tpm.sys
Start      = Kernel driver
Group      = Manual;Boot Bus Extender

Thu Aug 13 21:54:58 2015Z
Name       = SecureLine
Display    = Avast SecureLine
ImagePath  = C:\Program Files\AVAST Software\SecureLine\VpnSvc.exe
Type       = Own_Process
Start      = Auto Start
Group      =

Thu Aug 13 21:54:41 2015Z
Name       = 3ware
Display    =
ImagePath  = System32\drivers\3ware.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI miniport

Name       = ADP80XX
Display    =
ImagePath  = System32\drivers\ADP80XX.SYS
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Miniport

Name       = agp440
Display    = @machine.inf,%agp440_svcdesc%
ImagePath  = Intel AGP Bus Filter
Type       = System32\drivers\agp440.sys
Start      = Kernel driver
Group      = Boot Start;PnP Filter

Name       = amdsata
Display    =
ImagePath  = System32\drivers\amdsata.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI miniport

Name       = amdsbs
Display    =
ImagePath  = System32\drivers\amdsbs.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI miniport

Name       = amdxata
Display    =
ImagePath  = System32\drivers\amdxata.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI miniport
```

Page 43

SYSTEM OUTPUT.txt

```
Name       = arcsas
Display    = @arcsas.inf,%arcsas_ServiceName%
ImagePath  = Adaptec SAS/SATA-II RAID Storport's Miniport Driver
Type       = System32\drivers\arcsas.sys
Start      = Kernel driver
Group      = Boot Start;SCSI miniport

Name       = atapi
Display    = @mshdc.inf,%idechannel.DeviceDesc%
ImagePath  = IDE Channel
Type       = System32\drivers\atapi.sys
Start      = Kernel driver
Group      = Boot Start;SCSI Miniport

Name       = b06bdrv
Display    = @netbvbda.inf,%vbd_srv_desc%
ImagePath  = Broadcom NetXtreme II VBD
Type       = System32\drivers\bxvbda.sys
Start      = Kernel driver
Group      = Boot Start;System Bus Extender

Name       = ebdrv
Display    = @netevbda.inf,%vbd_srv_desc%
ImagePath  = QLogic 10 Gigabit Ethernet Adapter VBD
Type       = System32\drivers\evbda.sys
Start      = Kernel driver
Group      = Boot Start;System Bus Extender

Name       = EhStorTcgDrv
Display    = @ehstortcgdrv.inf,%EhStorTcgDrv.Desc%
ImagePath  = Microsoft driver for storage devices supporting IEEE 1667 and TCG
protocols
Type       = System32\drivers\EhStorTcgDrv.sys
Start      = Kernel driver
Group      = Boot Start;SCSI Class

Name       = gagp30kx
Display    = @machine.inf,%gagp30kx_svcdesc%
ImagePath  = Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms
Type       = System32\drivers\gagp30kx.sys
Start      = Kernel driver
Group      = Boot Start;PnP Filter

Name       = HpSAMD
Display    =
ImagePath  = System32\drivers\HpSAMD.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Miniport

Name       = iaStorAV
Display    = @iastorav.inf,%iaStorAV.DeviceDesc%
ImagePath  = Intel(R) SATA RAID Controller Windows
Type       = System32\drivers\iaStorAV.sys
Start      = Kernel driver
Group      = Boot Start;SCSI miniport

Name       = iaStorV
Display    = @iastorv.inf,%*PNP0600.DeviceDesc%
ImagePath  = Intel RAID Controller Windows 7
Type       = System32\drivers\iaStorV.sys
Start      = Kernel driver
```

Page 44

```
                                    SYSTEM OUTPUT.txt
Group        = Boot Start;SCSI Miniport

Name         = intelide
Display      =
ImagePath    = System32\drivers\intelide.sys
Type         = Kernel driver
Start        = Boot Start
Group        = System Bus Extender

Name         = isapnp
Display      =
ImagePath    = System32\drivers\isapnp.sys
Type         = Kernel driver
Start        = Boot Start
Group        = Boot Bus Extender

Name         = LSI_SAS
Display      =
ImagePath    = System32\drivers\lsi_sas.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = LSI_SAS2i
Display      =
ImagePath    = System32\drivers\lsi_sas2i.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = LSI_SAS3i
Display      =
ImagePath    = System32\drivers\lsi_sas3i.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = LSI_SSS
Display      =
ImagePath    = System32\drivers\lsi_sss.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = megasas
Display      =
ImagePath    = System32\drivers\megasas.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = megasr
Display      =
ImagePath    = System32\drivers\megasr.sys
Type         = Kernel driver
Start        = Boot Start
Group        = SCSI Miniport

Name         = mvumis
Display      =
ImagePath    = System32\drivers\mvumis.sys
Type         = Kernel driver
Start        = Boot Start
```

Page 45

SYSTEM OUTPUT.txt

```
Group       = SCSI Miniport

Name        = nvraid
Display     =
ImagePath   = System32\drivers\nvraid.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Bus Extender

Name        = nvstor
Display     =
ImagePath   = System32\drivers\nvstor.sys
Type        = Kernel driver
Start       = Boot Start
Group       = SCSI Miniport

Name        = nv_agp
Display     = @machine.inf,%agpnvidia_svcdesc%
ImagePath   = NVIDIA nForce AGP Bus Filter
Type        = System32\drivers\nv_agp.sys
Start       = Kernel driver
Group       = Boot Start;PnP Filter

Name        = pciide
Display     =
ImagePath   = System32\drivers\pciide.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Bus Extender

Name        = pcmcia
Display     =
ImagePath   = System32\drivers\pcmcia.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Bus Extender

Name        = percsas2i
Display     =
ImagePath   = System32\drivers\percsas2i.sys
Type        = Kernel driver
Start       = Boot Start
Group       = SCSI Miniport

Name        = percsas3i
Display     =
ImagePath   = System32\drivers\percsas3i.sys
Type        = Kernel driver
Start       = Boot Start
Group       = SCSI Miniport

Name        = sbp2port
Display     = @sbp2.inf,%sbp2_ServiceDesc%
ImagePath   = SBP-2 Transport/Protocol Bus Driver
Type        = System32\drivers\sbp2port.sys
Start       = Kernel driver
Group       = Boot Start;

Name        = SiSRaid2
Display     =
ImagePath   = System32\drivers\SiSRaid2.sys
Type        = Kernel driver
Start       = Boot Start
```

Page 46

```
                              SYSTEM OUTPUT.txt
Group      = SCSI Miniport

Name       = SiSRaid4
Display    =
ImagePath  = System32\drivers\sisraid4.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Miniport

Name       = stexstor
Display    =
ImagePath  = System32\drivers\stexstor.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Miniport

Name       = storflt
Display    = @wstorflt.inf,%service_desc%
ImagePath  = Microsoft Hyper-V Storage Accelerator
Type       = System32\drivers\vmstorfl.sys
Start      = Kernel driver
Group      = Boot Start;Extended Base

Name       = storufs
Display    = @storufs.inf,%UfsServiceDesc%
ImagePath  = Microsoft Universal Flash Storage (UFS) Driver
Type       = System32\drivers\storufs.sys
Start      = Kernel driver
Group      = Boot Start;

Name       = storvsc
Display    =
ImagePath  = System32\drivers\storvsc.sys
Type       = Kernel driver
Start      = Boot Start
Group      = Base

Name       = uagp35
Display    = @machine.inf,%uagp35_svcdesc%
ImagePath  = Microsoft AGPv3.5 Filter
Type       = System32\drivers\uagp35.sys
Start      = Kernel driver
Group      = Boot Start;PnP Filter

Name       = uliagpkx
Display    = @machine.inf,%uliagpkx_svcdesc%
ImagePath  = Uli AGP Bus Filter
Type       = System32\drivers\uliagpkx.sys
Start      = Kernel driver
Group      = Boot Start;PnP Filter

Name       = vmbus
Display    = @wvmbus.inf,%vmbus.SVCDESC%
ImagePath  = Virtual Machine Bus
Type       = System32\drivers\vmbus.sys
Start      = Kernel driver
Group      = Boot Start;System Bus Extender

Name       = vsmraid
Display    =
ImagePath  = System32\drivers\vsmraid.sys
Type       = Kernel driver
Start      = Boot Start
```

Page 47

```
                              SYSTEM OUTPUT.txt
    Group       = SCSI Miniport

    Name        = VSTXRAID
    Display     = @vstxraid.inf,%Driver.DeviceDesc%
    ImagePath   = VIA StorX Storage RAID Controller Windows Driver
    Type        = System32\drivers\vstxraid.sys
    Start       = Kernel driver
    Group       = Boot Start;SCSI Miniport

Thu Jul 16 04:12:19 2015Z
    Name        = WINUSB
    Display     = @winusb.inf,%WINUSB_SvcDesc%
    ImagePath   = WinUsb Driver
    Type        = \SystemRoot\System32\drivers\WinUSB.SYS
    Start       = Kernel driver
    Group       = Manual;

Thu Jul 16 04:12:16 2015Z
    Name        = terminpt
    Display     = @termmou.inf,%TermInpt.SVCDESC%
    ImagePath   = Microsoft Remote Desktop Input Driver
    Type        = \SystemRoot\System32\drivers\terminpt.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

Thu Jul 16 04:12:01 2015Z
    Name        = kbdhid
    Display     = @keyboard.inf,%KBDHID.SvcDesc%
    ImagePath   = Keyboard HID Driver
    Type        = \SystemRoot\System32\drivers\kbdhid.sys
    Start       = Kernel driver
    Group       = Manual;

Thu Jul 16 04:11:59 2015Z
    Name        = WUDFRd
    Display     = @hidbthle.inf,%WudfRdDisplayName%
    ImagePath   = Windows Driver Foundation - User-mode Driver Framework Reflector
    Type        = \SystemRoot\System32\drivers\WUDFRd.sys
    Start       = Kernel driver
    Group       = Manual;Base

Thu Jul 16 04:01:46 2015Z
    Name        = TabletInputService
    Display     = @%SystemRoot%\system32\TabSvc.dll,-100
    ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
    Type        = Share_Process
    Start       = Manual
    Group       = PlugPlay

Thu Jul 16 03:47:02 2015Z
    Name        = UEIPSvc
    Display     = User Experience Improvement Program
    ImagePath   = "C:\Program Files\Acer\User Experience Improvement
Program\Framework\UBTService.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Jul 16 03:46:19 2015Z
    Name        = MozillaMaintenance
    Display     = Mozilla Maintenance Service
    ImagePath   = "C:\Program Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe"
                              Page 48
```

SYSTEM OUTPUT.txt
```
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Jul 16 03:44:48 2015Z
    Name        = GamesAppIntegrationService
    Display     = GamesAppIntegrationService
    ImagePath = "C:\Program Files (x86)\WildTangent
Games\App\GamesAppIntegrationService.exe"
    Type        = Own_Process
    Start       = Auto Start
    Group       =

Thu Jul 16 03:44:47 2015Z
    Name        = GamesAppService
    Display     = GamesAppService
    ImagePath = "C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe"
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Jul 16 03:41:07 2015Z
    Name        = FontCache3.0.0.0
    Display     = @%SystemRoot%\system32\PresentationHost.exe,-3309
    ImagePath =
%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

Thu Jul 16 03:40:55 2015Z
    Name        = .NET CLR Data
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = .NET CLR Networking
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = clr_optimization_v2.0.50727_32
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

    Name        = clr_optimization_v2.0.50727_64
    Display     =
    ImagePath =
    Type        =
    Start       =
    Group       =

Thu Jul 16 03:34:32 2015Z
    Name        = PrintNotify
    Display     = @C:\windows\system32\spool\drivers\x64\3\PrintConfig.dll,-1
    ImagePath = %SystemRoot%\system32\svchost.exe -k print
```
Page 49

SYSTEM OUTPUT.txt

```
    Type        = 0x0
    Start       = Manual
    Group       =

Thu Jul 16 03:32:44 2015Z
    Name        = NativeWifiP
    Display     = @%SystemRoot%\System32\drivers\nwifi.sys,-101
    ImagePath   = system32\DRIVERS\nwifi.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = NDIS

Thu Jul 16 03:31:44 2015Z
    Name        = GPIOClx0101
    Display     = Microsoft GPIO Class Extension Driver
    ImagePath   = System32\Drivers\msgpioclx.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = System Bus Extender

    Name        = SpbCx
    Display     = Simple Peripheral Bus Support Library
    ImagePath   = system32\drivers\SpbCx.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

Fri Jul 10 13:14:47 2015Z
    Name        = RDPDR
    Display     = @%SystemRoot%\System32\DRIVERS\rdpdr.sys,-100
    ImagePath   = System32\drivers\rdpdr.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

    Name        = RdpVideoMiniport
    Display     = Remote Desktop Video Miniport Driver
    ImagePath   = System32\drivers\rdpvideominiport.sys
    Type        = Kernel driver
    Start       = Manual
    Group       =

    Name        = SensrSvc
    Display     = @%SystemRoot%\System32\sensrsvc.dll,-1000
    ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
    Type        = Share_Process
    Start       = Manual
    Group       =

    Name        = UmRdpService
    Display     = @%SystemRoot%\system32\umrdp.dll,-1000
    ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
    Type        = Share_Process
    Start       = Manual
    Group       =

Fri Jul 10 13:14:46 2015Z
    Name        = RDPUDD
    Display     =
    ImagePath   =
    Type        =
    Start       =
    Group       =
```

Page 50

SYSTEM OUTPUT.txt

```
Fri Jul 10 12:22:48 2015Z
    Name      = Synth3dVsc
    Display   =
    ImagePath = \SystemRoot\System32\drivers\Synth3dVsc.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

Fri Jul 10 12:22:47 2015Z
    Name      = dmvsc
    Display   =
    ImagePath = \SystemRoot\System32\drivers\dmvsc.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

    Name      = gencounter
    Display   = @wgencounter.inf,%GenCounter.SVCDESC%
    ImagePath = Microsoft Hyper-V Generation Counter
    Type      = \SystemRoot\System32\drivers\vmgencounter.sys
    Start     = Kernel driver
    Group     = Manual;

Fri Jul 10 12:22:44 2015Z
    Name      = UASPStor
    Display   = @uaspstor.inf,%UASPortName%
    ImagePath = USB Attached SCSI (UAS) Driver
    Type      = \SystemRoot\System32\drivers\uaspstor.sys
    Start     = Kernel driver
    Group     = Manual;

Fri Jul 10 12:22:43 2015Z
    Name      = sdstor
    Display   = @sdstor.inf,%sdstor_ServiceDesc%
    ImagePath = SD Storage Port Driver
    Type      = \SystemRoot\System32\drivers\sdstor.sys
    Start     = Kernel driver
    Group     = Manual;

Fri Jul 10 12:22:41 2015Z
    Name      = npsvctrig
    Display   = @npsvctrig.inf,%NPSVCTRIG.SvcDisplayName%
    ImagePath = Named pipe service trigger provider
    Type      = \SystemRoot\System32\drivers\npsvctrig.sys
    Start     = Kernel driver
    Group     = System Start;

Fri Jul 10 12:22:39 2015Z
    Name      = AsyncMac
    Display   = @%systemroot%\system32\rascfg.dll,-32000
    ImagePath = \SystemRoot\System32\drivers\asyncmac.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =

Fri Jul 10 12:22:25 2015Z
    Name      = IPMIDRV
    Display   =
    ImagePath = \SystemRoot\System32\drivers\IPMIDrv.sys
    Type      = Kernel driver
    Start     = Manual
    Group     =
```

Page 51

SYSTEM OUTPUT.txt

```
Name        = iScsiPrt
Display     = @iscsi.inf,%iScsiPortName%
ImagePath   = iScsiPort Driver
Type        = \SystemRoot\System32\drivers\msiscsi.sys
Start       = Kernel driver
Group       = Manual;

Fri Jul 10 12:22:22 2015Z
Name        = HidBatt
Display     = @hidbatt.inf,%HidBatt.SvcDesc%
ImagePath   = HID UPS Battery Driver
Type        = \SystemRoot\System32\drivers\HidBatt.sys
Start       = Kernel driver
Group       = Manual;

Name        = mshidumdf
Display     = @%SystemRoot%\system32\drivers\mshidumdf.sys,-100
ImagePath   = \SystemRoot\System32\drivers\mshidumdf.sys
Type        = Kernel driver
Start       = Manual
Group       = Base

Fri Jul 10 12:22:21 2015Z
Name        = fdc
Display     = @fdc.inf,%fdc_ServiceDesc%
ImagePath   = Floppy Disk Controller Driver
Type        = \SystemRoot\System32\drivers\fdc.sys
Start       = Kernel driver
Group       = Manual;

Name        = flpydisk
Display     = @flpydisk.inf,%floppy_ServiceDesc%
ImagePath   = Floppy Disk Driver
Type        = \SystemRoot\System32\drivers\flpydisk.sys
Start       = Kernel driver
Group       = Manual;

Name        = sfloppy
Display     = @flpydisk.inf,%sfloppy_devdesc%
ImagePath   = High-Capacity Floppy Disk Drive
Type        = \SystemRoot\System32\drivers\sfloppy.sys
Start       = Kernel driver
Group       = Manual;

Fri Jul 10 12:22:20 2015Z
Name        = CapImg
Display     = @capimg.inf,%CapImgHid_Service%
ImagePath   = HID driver for CapImg touch screen
Type        = \SystemRoot\System32\drivers\capimg.sys
Start       = Kernel driver
Group       = Manual;

Fri Jul 10 12:22:19 2015Z
Name        = BTHMODEM
Display     = @bthspp.inf,%BthSerial.DisplayName%
ImagePath   = Bluetooth Serial Communications Driver
Type        = \SystemRoot\System32\drivers\bthmodem.sys
Start       = Kernel driver
Group       = Manual;

Fri Jul 10 12:22:18 2015Z
Name        = bthhfhid
```

Page 52

```
                         SYSTEM OUTPUT.txt
Display    = @bthaudhid.inf,%BthAudioHFHid.SVCDESC%
ImagePath = Bluetooth Hands-Free Call Control HID
Type       = \SystemRoot\System32\drivers\BthHFHid.sys
Start      = Kernel driver
Group      = Manual;

Fri Jul 10 12:22:16 2015z
Name       = 1394ohci
Display    = @1394.inf,%PCI\CC_0C0010.DeviceDesc%
ImagePath = 1394 OHCI Compliant Host Controller
Type       = \SystemRoot\System32\drivers\1394ohci.sys
Start      = Kernel driver
Group      = Manual;

Name       = AcpiPmi
Display    = @acpipmi.inf,%AcpiPmi.SvcDesc%
ImagePath = ACPI Power Meter Driver
Type       = \SystemRoot\System32\drivers\acpipmi.sys
Start      = Kernel driver
Group      = Manual;

Fri Jul 10 12:22:08 2015z
Name       = wuauserv
Display    = @%systemroot%\system32\wuaueng.dll,-105
ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
Type       = Share_Process
Start      = Manual
Group      =

Fri Jul 10 12:21:44 2015z
Name       = iphlpsvc
Display    = @%SystemRoot%\system32\iphlpsvc.dll,-500
ImagePath = %SystemRoot%\System32\svchost.exe -k NetSvcs
Type       = Share_Process
Start      = Auto Start
Group      =

Name       = LanmanServer
Display    = @%systemroot%\system32\srvsvc.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type       = Share_Process
Start      = Auto Start
Group      =

Fri Jul 10 12:21:43 2015z
Name       = PEAUTH
Display    = PEAUTH
ImagePath = system32\drivers\peauth.sys
Type       = Kernel driver
Start      = Auto Start
Group      =

Name       = srvnet
Display    =
ImagePath = System32\DRIVERS\srvnet.sys
Type       = File system driver
Start      = Manual
Group      = Network

Fri Jul 10 12:21:42 2015z
Name       = MsLldp
Display    = @%SystemRoot%\system32\drivers\mslldp.sys,-200
ImagePath = system32\drivers\mslldp.sys
```

                              Page 53

SYSTEM OUTPUT.txt

```
Type        = Kernel driver
Start       = Auto Start
Group       = NDIS

Fri Jul 10 12:21:37 2015Z
  Name        = crypt32
  Display     =
  ImagePath =
  Type        =
  Start       =
  Group       =

Fri Jul 10 12:21:24 2015Z
  Name        = hyperkbd
  Display     =
  ImagePath = \SystemRoot\System32\drivers\hyperkbd.sys
  Type        = Kernel driver
  Start       = Manual
  Group       = Extended Base

  Name        = HyperVideo
  Display     =
  ImagePath = \SystemRoot\system32\DRIVERS\HyperVideo.sys
  Type        = Kernel driver
  Start       = Manual
  Group       = Video

  Name        = netvsc
  Display     =
  ImagePath = \SystemRoot\System32\drivers\netvsc.sys
  Type        = Kernel driver
  Start       = Manual
  Group       = Extended Base

  Name        = s3cap
  Display     =
  ImagePath = \SystemRoot\System32\drivers\vms3cap.sys
  Type        = Kernel driver
  Start       = Manual
  Group       = Video

  Name        = VMBusHID
  Display     =
  ImagePath = \SystemRoot\System32\drivers\VMBusHID.sys
  Type        = Kernel driver
  Start       = Manual
  Group       = Extended Base

Fri Jul 10 12:21:21 2015Z
  Name        = cnghwassist
  Display     = @%SystemRoot%\system32\drivers\cnghwassist.sys,-100
  ImagePath = System32\DRIVERS\cnghwassist.sys
  Type        = Kernel driver
  Start       = Disabled
  Group       = Base

Fri Jul 10 12:20:51 2015Z
  Name        = NETVSCVFPP
  Display     =
  ImagePath =
  Type        =
  Start       =
  Group       =
```

Page 54

SYSTEM OUTPUT.txt

```
Fri Jul 10 12:20:44 2015Z
    Name       = NetSetupSvc
    Display    = @%SystemRoot%\system32\NetSetupSvc.dll,-3
    ImagePath  = %SystemRoot%\System32\svchost.exe -k netsvcs
    Type       = Share_Process
    Start      = Manual
    Group      =

Fri Jul 10 12:20:30 2015Z
    Name       = Psched
    Display    = @%windir%\System32\drivers\pacer.sys,-101
    ImagePath  = System32\drivers\pacer.sys
    Type       = Kernel driver
    Start      = System Start
    Group      = NDIS

    Name       = vwififlt
    Display    = @%SystemRoot%\System32\drivers\vwififlt.sys,-259
    ImagePath  = System32\drivers\vwififlt.sys
    Type       = Kernel driver
    Start      = System Start
    Group      = NDIS

Fri Jul 10 12:20:26 2015Z
    Name       = Tcpip
    Display    = @%SystemRoot%\system32\tcpipcfg.dll,-50003
    ImagePath  = System32\drivers\tcpip.sys
    Type       = Kernel driver
    Start      = Boot Start
    Group      = PNP_TDI

    Name       = Tcpip6
    Display    = @todo.dll,-100
    ImagePath  = Microsoft IPv6 Protocol Driver
    Type       = System32\drivers\tcpip.sys
    Start      = Kernel driver
    Group      = Manual;

    Name       = TCPIP6TUNNEL
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = TCPIPTUNNEL
    Display    =
    ImagePath  =
    Type       =
    Start      =
    Group      =

    Name       = WFPLWFS
    Display    = @%SystemRoot%\System32\drivers\wfplwfs.sys,-6000
    ImagePath  = System32\drivers\wfplwfs.sys
    Type       = Kernel driver
    Start      = Boot Start
    Group      = PNP_TDI

Fri Jul 10 12:20:23 2015Z
    Name       = acpiex
    Display    = Microsoft ACPIEx Driver
```

Page 55

```
                          SYSTEM OUTPUT.txt
ImagePath = System32\Drivers\acpiex.sys
Type      = Kernel driver
Start     = Boot Start
Group     = Boot Bus Extender

Name      = Ucx01000
Display   = USB Host Support Library
ImagePath = system32\drivers\ucx01000.sys
Type      = Kernel driver
Start     = Manual
Group     = Boot Bus Extender

Name      = WindowsTrustedRT
Display   = Windows Trusted Execution Environment Class Extension
ImagePath = system32\drivers\WindowsTrustedRT.sys
Type      = Kernel driver
Start     = Boot Start
Group     = Core Security Extensions

Name      = WindowsTrustedRTProxy
Display   = @WindowsTrustedRTProxy.inf,%WindowsTrustedRTProxy.SVCDESC%
ImagePath = Microsoft Windows Trusted Runtime Secure Service
Type      = System32\drivers\WindowsTrustedRTProxy.sys
Start     = Kernel driver
Group     = Boot Start;Core Security Extensions

Fri Jul 10 11:06:22 2015Z
Name      = AudioEndpointBuilder
Display   = @%SystemRoot%\system32\AudioEndpointBuilder.dll,-204
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     = AudioGroup

Name      = Audiosrv
Display   = @%SystemRoot%\system32\audiosrv.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     = AudioGroup

Name      = MMCSS
Display   = @%systemroot%\system32\drivers\mmcss.sys,-100
ImagePath = \SystemRoot\system32\drivers\mmcss.sys
Type      = Kernel driver
Start     = Auto Start
Group     =

Fri Jul 10 11:06:01 2015Z
Name      = Winsock
Display   =
ImagePath =
Type      =
Start     =
Group     =

Fri Jul 10 11:05:46 2015Z
Name      = LanmanWorkstation
Display   = @%systemroot%\system32\wkssvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService
Type      = Share_Process
Start     = Auto Start
Group     = NetworkProvider
```
                              Page 56

SYSTEM OUTPUT.txt

```
Name       = NdisImPlatform
Display    = @%SystemRoot%\System32\drivers\ndisimplatform.sys,-501
ImagePath  = System32\drivers\NdisImPlatform.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = NetBIOS
Display    = @%windir%\system32\drivers\netbios.sys,-503
ImagePath  = system32\drivers\netbios.sys
Type       = File system driver
Start      = System Start
Group      = NetBIOSGroup

Name       = NetbiosSmb
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = RDMANDK
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Fri Jul 10 11:05:25 2015z
Name       = AFD
Display    = @%systemroot%\system32\drivers\afd.sys,-1000
ImagePath  = \SystemRoot\system32\drivers\afd.sys
Type       = Kernel driver
Start      = System Start
Group      = PNP_TDI

Name       = ahcache
Display    = @%systemroot%\system32\drivers\ahcache.sys,-102
ImagePath  = system32\DRIVERS\ahcache.sys
Type       = Kernel driver
Start      = System Start
Group      =

Name       = AJRouter
Display    = @%SystemRoot%\system32\AJRouter.dll,-2
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalService
Type       = Share_Process
Start      = Manual
Group      =

Name       = ALG
Display    = @%SystemRoot%\system32\Alg.exe,-112
ImagePath  = %SystemRoot%\System32\alg.exe
Type       = Own_Process
Start      = Manual
Group      =

Name       = AppID
Display    = @%systemroot%\system32\srpapi.dll,-100
ImagePath  = \SystemRoot\system32\drivers\appid.sys
Type       = Kernel driver
Start      = Manual
```

Page 57

```
                          SYSTEM OUTPUT.txt
Group      =

Name       = AppIDSvc
Display    = @%systemroot%\system32\appidsvc.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      = ProfSvc_Group

Name       = Appinfo
Display    = @%systemroot%\system32\appinfo.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k netsvcs
Type       = Share_Process
Start      = Manual
Group      =

Name       = AppReadiness
Display    = @%SystemRoot%\System32\AppReadiness.dll,-1000
ImagePath  = %SystemRoot%\System32\svchost.exe -k AppReadiness
Type       = Share_Process
Start      = Manual
Group      =

Name       = AppXSvc
Display    = @%SystemRoot%\system32\appxdeploymentserver.dll,-1
ImagePath  = %systemroot%\system32\svchost.exe -k wsappx
Type       = Share_Process
Start      = Manual
Group      =

Name       = AxInstSV
Display    = @%SystemRoot%\system32\AxInstSV.dll,-103
ImagePath  = %SystemRoot%\system32\svchost.exe -k AxInstSVGroup
Type       = Share_Process
Start      = Manual
Group      =

Name       = BDESVC
Display    = @%SystemRoot%\system32\bdesvc.dll,-100
ImagePath  = %SystemRoot%\System32\svchost.exe -k netsvcs
Type       = Share_Process
Start      = Manual
Group      =

Name       = Beep
Display    = Beep
ImagePath  =
Type       = Kernel driver
Start      = System Start
Group      = Base

Name       = BFE
Display    = @%SystemRoot%\system32\bfe.dll,-1001
ImagePath  = %systemroot%\system32\svchost.exe -k LocalServiceNoNetwork
Type       = Share_Process
Start      = Auto Start
Group      = NetworkProvider

Name       = bowser
Display    = @%systemroot%\system32\browser.dll,-102
ImagePath  = system32\DRIVERS\bowser.sys
Type       = File system driver
Start      = Manual
```

Page 58

SYSTEM OUTPUT.txt

```
Group       = Network

Name        = BrokerInfrastructure
Display     = @%windir%\system32\bisrv.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type        = Share_Process
Start       = Auto Start
Group       = COM Infrastructure

Name        = Browser
Display     = @%systemroot%\system32\browser.dll,-100
ImagePath   = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       = NetworkProvider

Name        = bthserv
Display     = @%SystemRoot%\System32\bthserv.dll,-101
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = cdfs
Display     = CD/DVD File System Reader
ImagePath   = system32\DRIVERS\cdfs.sys
Type        = File system driver
Start       = Disabled
Group       = Boot File System

Name        = CDPSvc
Display     = @%SystemRoot%\system32\cdpsvc.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = CertPropSvc
Display     = @%SystemRoot%\System32\certprop.dll,-11
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = CLFS
Display     = @%SystemRoot%\system32\drivers\clfs.sys,-100
ImagePath   = System32\drivers\CLFS.sys
Type        = Kernel driver
Start       = Boot Start
Group       = Filter

Name        = ClipSVC
Display     = @%SystemRoot%\system32\ClipSVC.dll,-103
ImagePath   = %SystemRoot%\System32\svchost.exe -k wsappx
Type        = Share_Process
Start       = Manual
Group       =

Name        = CNG
Display     =
ImagePath   = System32\Drivers\cng.sys
Type        = Kernel driver
Start       = Boot Start
```

Page 59

```
                         SYSTEM OUTPUT.txt
     Group         = Core

     Name          = COMSysApp
     Display       = @comres.dll,-947
     ImagePath = %SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
     Type          = Own_Process
     Start         = Manual
     Group         =

     Name          = condrv
     Display       = Console Driver
     ImagePath = System32\drivers\condrv.sys
     Type          = Kernel driver
     Start         = Manual
     Group         = Base

     Name          = CoreMessagingRegistrar
     Display       = @%SystemRoot%\system32\coremessaging.dll,-1
     ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork
     Type          = Share_Process
     Start         = Auto Start
     Group         =

     Name          = CryptSvc
     Display       = @%SystemRoot%\system32\cryptsvc.dll,-1001
     ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkService
     Type          = Share_Process
     Start         = Auto Start
     Group         =

     Name          = dam
     Display       = @%SystemRoot%\system32\drivers\dam.sys,-100
     ImagePath = system32\drivers\dam.sys
     Type          = Kernel driver
     Start         = System Start
     Group         =

     Name          = DcomLaunch
     Display       = @combase.dll,-5012
     ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch
     Type          = Share_Process
     Start         = Auto Start
     Group         = COM Infrastructure

     Name          = DcpSvc
     Display       = @%SystemRoot%\system32\dcpsvc.dll,-3001
     ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
     Type          = Share_Process
     Start         = Manual
     Group         =

     Name          = defragsvc
     Display       = @%SystemRoot%\system32\defragsvc.dll,-101
     ImagePath = %SystemRoot%\system32\svchost.exe -k defragsvc
     Type          = Own_Process
     Start         = Manual
     Group         =

     Name          = DeviceInstall
     Display       = @%SystemRoot%\system32\umpnpmgr.dll,-100
     ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch
     Type          = Share_Process
```

Page 60

```
                         SYSTEM OUTPUT.txt
    Start       = Manual
    Group       = PlugPlay

    Name        = DevQueryBroker
    Display     = @%SystemRoot%\system32\DevQueryBroker.dll,-100
    ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
    Type        = Share_Process
    Start       = Manual
    Group       =

    Name        = Dfsc
    Display     = @%systemroot%\system32\wkssvc.dll,-1008
    ImagePath   = System32\Drivers\dfsc.sys
    Type        = File system driver
    Start       = System Start
    Group       = Network

    Name        = Dhcp
    Display     = @%SystemRoot%\system32\dhcpcore.dll,-100
    ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
    Type        = Share_Process
    Start       = Auto Start
    Group       = TDI

    Name        = diagnosticshub.standardcollector.service
    Display     =
@%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-100
0
    ImagePath   =
%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe
    Type        = Own_Process
    Start       = Manual
    Group       =

    Name        = DiagTrack
    Display     = @%SystemRoot%\system32\diagtrack.dll,-3001
    ImagePath   = %SystemRoot%\System32\svchost.exe -k utcsvc
    Type        = Own_Process
    Start       = Auto Start
    Group       =

    Name        = DmEnrollmentSvc
    Display     = @%systemroot%\system32\Windows.Internal.Management.dll,-100
    ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
    Type        = Own_Process
    Start       = Manual
    Group       =

    Name        = dmwappushservice
    Display     = @%SystemRoot%\system32\dmwappushsvc.dll,-200
    ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
    Type        = Share_Process
    Start       = Auto Start
    Group       =

    Name        = Dnscache
    Display     = @%SystemRoot%\System32\dnsapi.dll,-101
    ImagePath   = %SystemRoot%\system32\svchost.exe -k NetworkService
    Type        = Share_Process
    Start       = Auto Start
    Group       = TDI

    Name        = DoSvc
                                Page 61
```

```
                            SYSTEM OUTPUT.txt
Display     = @%systemroot%\system32\dosvc.dll,-100
ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = dot3svc
Display     = @%systemroot%\system32\dot3svc.dll,-1102
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       = TDI

Name        = DPS
Display     = @%systemroot%\system32\dps.dll,-500
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = DsmSvc
Display     = @%SystemRoot%\system32\DeviceSetupManager.dll,-1000
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = DsSvc
Display     = @%SystemRoot%\system32\dssvc.dll,-10003
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = DXGKrnl
Display     = LDDM Graphics Subsystem
ImagePath = \SystemRoot\System32\drivers\dxgkrnl.sys
Type        = Kernel driver
Start       = Manual
Group       = Video Init

Name        = Eaphost
Display     = @%systemroot%\system32\eapsvc.dll,-1
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = EFS
Display     = @%SystemRoot%\system32\efssvc.dll,-100
ImagePath = %SystemRoot%\System32\lsass.exe
Type        = Share_Process
Start       = Manual
Group       =

Name        = embeddedmode
Display     = @%SystemRoot%\system32\embeddedmodesvc.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = EntAppSvc
```

                                Page 62

```
                              SYSTEM OUTPUT.txt
Display    = @EnterpriseAppMgmtSvc.dll,-1
ImagePath  = %systemroot%\system32\svchost.exe -k appmodel
Type       = Share_Process
Start      = Manual
Group      =

Name       = EventSystem
Display    = @comres.dll,-2450
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalService
Type       = Share_Process
Start      = Auto Start
Group      =

Name       = exfat
Display    = exFAT File System Driver
ImagePath  =
Type       = File system driver
Start      = Manual
Group      = Boot File System

Name       = fastfat
Display    = FAT12/16/32 File System Driver
ImagePath  =
Type       = File system driver
Start      = Manual
Group      = Boot File System

Name       = Fax
Display    = @%systemroot%\system32\fxsresm.dll,-118
ImagePath  = %systemroot%\system32\fxssvc.exe
Type       = Own_Process
Start      = Manual
Group      =

Name       = fdPHost
Display    = @%systemroot%\system32\fdPHost.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalService
Type       = Share_Process
Start      = Manual
Group      =

Name       = FDResPub
Display    = @%systemroot%\system32\fdrespub.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type       = Share_Process
Start      = Manual
Group      =

Name       = fhsvc
Display    = @%systemroot%\system32\fhsvc.dll,-101
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = FileCrypt
Display    = @%systemroot%\system32\drivers\filecrypt.sys,-100
ImagePath  = system32\drivers\filecrypt.sys
Type       = File system driver
Start      = System Start
Group      = FSFilter Encryption

Name       = FileInfo
```

Page 63

```
                         SYSTEM OUTPUT.txt
Display    = @%SystemRoot%\system32\drivers\fileinfo.sys,-100
ImagePath  = System32\drivers\fileinfo.sys
Type       = File system driver
Start      = Boot Start
Group      = FSFilter Bottom

Name       = Filetrace
Display    = @%SystemRoot%\system32\drivers\filetrace.sys,-10001
ImagePath  = system32\drivers\filetrace.sys
Type       = File system driver
Start      = Manual
Group      = FSFilter Activity Monitor

Name       = FltMgr
Display    = @%SystemRoot%\system32\drivers\fltmgr.sys,-10001
ImagePath  = system32\drivers\fltmgr.sys
Type       = File system driver
Start      = Boot Start
Group      = FSFilter Infrastructure

Name       = FontCache
Display    = @%systemroot%\system32\FntCache.dll,-100
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalService
Type       = Share_Process
Start      = Auto Start
Group      = AudioGroup

Name       = FsDepends
Display    = @%SystemRoot%\system32\drivers\fsdepends.sys,-10001
ImagePath  = System32\drivers\FsDepends.sys
Type       = File system driver
Start      = Manual
Group      = FSFilter Top

Name       = Fs_Rec
Display    =
ImagePath  =
Type       = 0x0
Start      = Boot Start
Group      = File System

Name       = gpsvc
Display    = @gpapi.dll,-112
ImagePath  = %systemroot%\system32\svchost.exe -k netsvcs
Type       = Share_Process
Start      = Auto Start
Group      = ProfSvc_Group

Name       = GpuEnergyDrv
Display    = @%SystemRoot%\system32\drivers\gpuenergydrv.sys,-100
ImagePath  = System32\drivers\gpuenergydrv.sys
Type       = Kernel driver
Start      = System Start
Group      =

Name       = hidserv
Display    = @%SystemRoot%\System32\hidserv.dll,-101
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = HomeGroupListener
```

Page 64

```
                                SYSTEM OUTPUT.txt
Display    = @%SystemRoot%\System32\ListSvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = HomeGroupProvider
Display    = @%SystemRoot%\System32\provsvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = HTTP
Display    = @%SystemRoot%\system32\drivers\http.sys,-1
ImagePath = system32\drivers\HTTP.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = hwpolicy
Display    = @%systemroot%\system32\drivers\hwpolicy.sys,-101
ImagePath = System32\drivers\hwpolicy.sys
Type       = Kernel driver
Start      = Boot Start
Group      =

Name       = icssvc
Display    = @%SystemRoot%\System32\tetheringservice.dll,-4097
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      = TDI

Name       = IEEtwCollectorService
Display    = @%SystemRoot%\system32\ieetwcollectorres.dll,-1000
ImagePath = %SystemRoot%\system32\IEEtwCollector.exe /V
Type       = Own_Process
Start      = Manual
Group      =

Name       = IoQos
Display    = @%SystemRoot%\system32\drivers\ioqos.sys,-100
ImagePath = system32\drivers\ioqos.sys
Type       = File system driver
Start      = Manual
Group      =

Name       = IpFilterDriver
Display    = @%systemroot%\system32\rascfg.dll,-32013
ImagePath = system32\DRIVERS\ipfltdrv.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = IPNAT
Display    = IP Network Address Translator
ImagePath = System32\drivers\ipnat.sys
Type       = Kernel driver
Start      = Manual
Group      =

Name       = IRENUM
```

Page 65

```
                            SYSTEM OUTPUT.txt
Display     = @%SystemRoot%\system32\drivers\irenum.sys,-100
ImagePath   = system32\drivers\irenum.sys
Type        = Kernel driver
Start       = Manual
Group       =

Name        = KeyIso
Display     = @keyiso.dll,-100
ImagePath   = %SystemRoot%\system32\lsass.exe
Type        = Share_Process
Start       = Manual
Group       =

Name        = KSecDD
Display     =
ImagePath   = System32\Drivers\ksecdd.sys
Type        = Kernel driver
Start       = Boot Start
Group       = Base

Name        = KSecPkg
Display     =
ImagePath   = System32\Drivers\ksecpkg.sys
Type        = Kernel driver
Start       = Boot Start
Group       = Cryptography

Name        = KtmRm
Display     = @comres.dll,-2946
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkServiceAndNoImpersonation
Type        = Share_Process
Start       = Manual
Group       =

Name        = lfsvc
Display     = @%SystemRoot%\System32\lfsvc.dll,-1
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = LicenseManager
Display     = @%SystemRoot%\system32\licensemanagersvc.dll,-200
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = lltdsvc
Display     = @%SystemRoot%\system32\lltdres.dll,-1
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = lmhosts
Display     = @%SystemRoot%\system32\lmhsvc.dll,-101
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       = TDI

Name        = LSM
```

Page 66

```
                              SYSTEM OUTPUT.txt
Display    = @%windir%\system32\lsm.dll,-1001
ImagePath  = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type       = Share_Process
Start      = Auto Start
Group      = COM Infrastructure

Name       = luafv
Display    = @%systemroot%\system32\drivers\luafv.sys,-100
ImagePath  = \SystemRoot\system32\drivers\luafv.sys
Type       = File system driver
Start      = Auto Start
Group      = FSFilter Virtualization

Name       = MapsBroker
Display    = @%SystemRoot%\System32\moshost.dll,-100
ImagePath  = %SystemRoot%\System32\svchost.exe -k NetworkService
Type       = Own_Process
Start      = Auto Start
Group      = NetworkService

Name       = Modem
Display    =
ImagePath  = system32\drivers\modem.sys
Type       = Kernel driver
Start      = Manual
Group      = Extended base

Name       = mountmgr
Display    = @%SystemRoot%\system32\drivers\mountmgr.sys,-100
ImagePath  = System32\drivers\mountmgr.sys
Type       = Kernel driver
Start      = Boot Start
Group      = System Bus Extender

Name       = mpsdrv
Display    = @%SystemRoot%\system32\drivers\mpsdrv.sys,-23092
ImagePath  = System32\drivers\mpsdrv.sys
Type       = Kernel driver
Start      = Manual
Group      = network

Name       = MpsSvc
Display    = @%SystemRoot%\system32\FirewallAPI.dll,-23090
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork
Type       = Share_Process
Start      = Auto Start
Group      = NetworkProvider

Name       = MRxDAV
Display    = @%systemroot%\system32\webclnt.dll,-104
ImagePath  = \SystemRoot\system32\drivers\mrxdav.sys
Type       = File system driver
Start      = Manual
Group      =

Name       = mrxsmb
Display    = @%systemroot%\system32\wkssvc.dll,-1002
ImagePath  = system32\DRIVERS\mrxsmb.sys
Type       = File system driver
Start      = Manual
Group      = Network

Name       = mrxsmb10
```

Page 67

```
                              SYSTEM OUTPUT.txt
Display     = @%systemroot%\system32\wkssvc.dll,-1004
ImagePath   = system32\DRIVERS\mrxsmb10.sys
Type        = File system driver
Start       = Auto Start
Group       = Network

Name        = mrxsmb20
Display     = @%systemroot%\system32\wkssvc.dll,-1006
ImagePath   = system32\DRIVERS\mrxsmb20.sys
Type        = File system driver
Start       = Manual
Group       = Network

Name        = MSiSCSI
Display     = @%SystemRoot%\system32\iscsidsc.dll,-5000
ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       = iSCSI

Name        = msiserver
Display     = @%SystemRoot%\system32\msimsg.dll,-27
ImagePath   = %systemroot%\system32\msiexec.exe /V
Type        = Own_Process
Start       = Manual
Group       =

Name        = Mup
Display     = @%systemroot%\system32\drivers\mup.sys,-101
ImagePath   = System32\Drivers\mup.sys
Type        = File system driver
Start       = Boot Start
Group       = Network

Name        = NcaSvc
Display     = @%SystemRoot%\system32\ncasvc.dll,-3009
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetSvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = NcbService
Display     = @%SystemRoot%\system32\ncbservice.dll,-500
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = NcdAutoSetup
Display     = @%SystemRoot%\system32\NcdAutoSetup.dll,-100
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork
Type        = Share_Process
Start       = Manual
Group       =

Name        = NDIS
Display     = @%SystemRoot%\system32\drivers\ndis.sys,-200
ImagePath   = system32\drivers\ndis.sys
Type        = Kernel driver
Start       = Boot Start
Group       = NDIS Wrapper

Name        = NdisCap
```

Page 68

```
                            SYSTEM OUTPUT.txt
Display    = @%SystemRoot%\System32\drivers\ndiscap.sys,-5000
ImagePath  = System32\drivers\ndiscap.sys
Type       = Kernel driver
Start      = Manual
Group      = NDIS

Name       = Ndu
Display    = @%SystemRoot%\system32\drivers\Ndu.sys,-10001
ImagePath  = system32\drivers\Ndu.sys
Type       = Kernel driver
Start      = Auto Start
Group      =

Name       = NetBT
Display    = @%SystemRoot%\system32\drivers\netbt.sys,-2
ImagePath  = System32\DRIVERS\netbt.sys
Type       = Kernel driver
Start      = System Start
Group      = PNP_TDI

Name       = Netlogon
Display    = @%SystemRoot%\System32\netlogon.dll,-102
ImagePath  = %systemroot%\system32\lsass.exe
Type       = Share_Process
Start      = Manual
Group      = MS_WindowsRemoteValidation

Name       = Netman
Display    = @%SystemRoot%\system32\netman.dll,-109
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      =

Name       = netprofm
Display    = @%SystemRoot%\system32\netprofmsvc.dll,-202
ImagePath  = %SystemRoot%\System32\svchost.exe -k LocalService
Type       = Share_Process
Start      = Manual
Group      =

Name       = NetTcpPortSharing
Display    =
@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8201
ImagePath  = %systemroot%\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
Type       = Share_Process
Start      = Disabled
Group      =

Name       = NgcCtnrSvc
Display    = @%SystemRoot%\System32\NgcCtnrSvc.dll,-1
ImagePath  = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type       = Share_Process
Start      = Manual
Group      = Cryptography

Name       = NgcSvc
Display    = @%SystemRoot%\System32\ngcsvc.dll,-100
ImagePath  = %SystemRoot%\system32\lsass.exe
Type       = Share_Process
Start      = Manual
Group      = Cryptography
```

Page 69

SYSTEM OUTPUT.txt

```
Name        = NlaSvc
Display     = @%SystemRoot%\System32\nlasvc.dll,-1
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = nsi
Display     = @%SystemRoot%\system32\nsisvc.dll,-200
ImagePath   = %systemroot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = nsiproxy
Display     = @%SystemRoot%\system32\drivers\nsiproxy.sys,-2
ImagePath   = system32\drivers\nsiproxy.sys
Type        = Kernel driver
Start       = System Start
Group       =

Name        = NTFS
Display     =
ImagePath   =
Type        = File system driver
Start       = Manual
Group       = Boot File System

Name        = OneSyncSvc
Display     = @%SystemRoot%\system32\APHostRes.dll,-10002
ImagePath   = %SystemRoot%\system32\svchost.exe -k UnistackSvcGroup
Type        = 0x0
Start       = Auto Start
Group       =

Name        = p2pimsvc
Display     = @%SystemRoot%\system32\pnrpsvc.dll,-8004
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type        = Share_Process
Start       = Manual
Group       =

Name        = p2psvc
Display     = @%SystemRoot%\system32\p2psvc.dll,-8006
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type        = Share_Process
Start       = Manual
Group       =

Name        = PcaSvc
Display     = @%SystemRoot%\system32\pcasvc.dll,-1
ImagePath   = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = pcw
Display     = Performance Counters for Windows Driver
ImagePath   = System32\drivers\pcw.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Reserved
```

Page 70

SYSTEM OUTPUT.txt

```
Name        = pdc
Display     = @%SystemRoot%\system32\drivers\pdc.sys,-100
ImagePath   = system32\drivers\pdc.sys
Type        = Kernel driver
Start       = Boot Start
Group       = Boot Bus Extender

Name        = PerfHost
Display     = @%systemroot%\sysWow64\perfhost.exe,-2
ImagePath   = %SystemRoot%\SysWow64\perfhost.exe
Type        = Own_Process
Start       = Manual
Group       =

Name        = PimIndexMaintenanceSvc
Display     = @%SystemRoot%\system32\UserDataAccessRes.dll,-15001
ImagePath   = %SystemRoot%\system32\svchost.exe -k UnistackSvcGroup
Type        = 0x0
Start       = Manual
Group       =

Name        = pla
Display     = @%systemroot%\system32\pla.dll,-500
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork
Type        = Share_Process
Start       = Manual
Group       =

Name        = PlugPlay
Display     = @%SystemRoot%\system32\umpnpmgr.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type        = Share_Process
Start       = Manual
Group       = PlugPlay

Name        = PNRPAutoReg
Display     = @%SystemRoot%\system32\pnrpauto.dll,-8002
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type        = Share_Process
Start       = Manual
Group       =

Name        = PNRPsvc
Display     = @%SystemRoot%\system32\pnrpsvc.dll,-8000
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet
Type        = Share_Process
Start       = Manual
Group       =

Name        = PolicyAgent
Display     = @%SystemRoot%\System32\polstore.dll,-5010
ImagePath   = %SystemRoot%\system32\svchost.exe -k NetworkServiceNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = Power
Display     = @%SystemRoot%\system32\umpo.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type        = Share_Process
Start       = Auto Start
Group       = Plugplay
```

Page 71

```
                         SYSTEM OUTPUT.txt
Name      = ProfSvc
Display   = @%systemroot%\system32\profsvc.dll,-300
ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Auto Start
Group     = profsvc_group

Name      = QWAVE
Display   = @%SystemRoot%\system32\qwave.dll,-1
ImagePath = %windir%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Manual
Group     =

Name      = QWAVEdrv
Display   = @%SystemRoot%\system32\drivers\qwavedrv.sys,-1
ImagePath = \SystemRoot\system32\drivers\qwavedrv.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = RasAuto
Display   = @%Systemroot%\system32\rasauto.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = RasMan
Display   = @%Systemroot%\system32\rasmans.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = rdbss
Display   = @%systemroot%\system32\wkssvc.dll,-1000
ImagePath = system32\DRIVERS\rdbss.sys
Type      = File system driver
Start     = System Start
Group     = Network

Name      = ReFSv1
Display   =
ImagePath =
Type      = File system driver
Start     = Manual
Group     = Boot File System

Name      = RemoteAccess
Display   = @%Systemroot%\system32\mprdim.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Disabled
Group     =

Name      = RemoteRegistry
Display   = @regsvc.dll,-1
ImagePath = %SystemRoot%\system32\svchost.exe -k localService
Type      = Share_Process
Start     = Disabled
Group     =
```

Page 72

SYSTEM OUTPUT.txt

```
Name      = RetailDemo
Display   = @%SystemRoot%\System32\RDXService.dll,-256
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = RpcEptMapper
Display   = @%windir%\system32\RpcEpMap.dll,-1001
ImagePath = %SystemRoot%\system32\svchost.exe -k RPCSS
Type      = Share_Process
Start     = Auto Start
Group     = COM Infrastructure

Name      = RpcLocator
Display   = @%systemroot%\system32\Locator.exe,-2
ImagePath = %SystemRoot%\system32\locator.exe
Type      = Own_Process
Start     = Manual
Group     =

Name      = RpcSs
Display   = @combase.dll,-5010
ImagePath = %SystemRoot%\system32\svchost.exe -k rpcss
Type      = Share_Process
Start     = Auto Start
Group     = COM Infrastructure

Name      = SamSs
Display   = @%SystemRoot%\system32\samsrv.dll,-1
ImagePath = %SystemRoot%\system32\lsass.exe
Type      = Share_Process
Start     = Auto Start
Group     = MS_WindowsLocalValidation

Name      = SCardSvr
Display   = @%SystemRoot%\System32\SCardSvr.dll,-1
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Disabled
Group     = SmartCardGroup

Name      = ScDeviceEnum
Display   = @%SystemRoot%\System32\ScDeviceEnum.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = scfilter
Display   = @%SystemRoot%\System32\drivers\scfilter.sys,-11
ImagePath = System32\DRIVERS\scfilter.sys
Type      = Kernel driver
Start     = Manual
Group     = PnP Filter

Name      = Schedule
Display   = @%SystemRoot%\system32\schedsvc.dll,-100
ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Auto Start
Group     = SchedulerGroup
```

Page 73

```
                                    SYSTEM OUTPUT.txt
Name        = SCPolicySvc
Display     = @%SystemRoot%\System32\certprop.dll,-13
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =


Name        = SDRSVC
Display     = @%SystemRoot%\system32\sdrsvc.dll,-107
ImagePath   = %SystemRoot%\system32\svchost.exe -k SDRSVC
Type        = Own_Process
Start       = Manual
Group       =


Name        = seclogon
Display     = @%SystemRoot%\system32\seclogon.dll,-7001
ImagePath   = %windir%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =


Name        = SENS
Display     = @%SystemRoot%\system32\Sens.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Auto Start
Group       = ProfSvc_Group


Name        = SensorDataService
Display     = @%SystemRoot%\system32\SensorDataService.exe,-101
ImagePath   = %SystemRoot%\System32\SensorDataService.exe
Type        = Own_Process
Start       = Manual
Group       =


Name        = SensorService
Display     = @%SystemRoot%\System32\sensorservice.dll,-1000
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =


Name        = SerCx
Display     = Serial UART Support Library
ImagePath   = system32\drivers\SerCx.sys
Type        = Kernel driver
Start       = Manual
Group       =


Name        = SerCx2
Display     = Serial UART Support Library
ImagePath   = system32\drivers\SerCx2.sys
Type        = Kernel driver
Start       = Manual
Group       =


Name        = SessionEnv
Display     = @%SystemRoot%\System32\SessEnv.dll,-1026
ImagePath   = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =
```

Page 74

```
                          SYSTEM OUTPUT.txt
Name      = SharedAccess
Display   = @%SystemRoot%\system32\ipnathlp.dll,-106
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = ShellHWDetection
Display   = @%SystemRoot%\System32\shsvcs.dll,-12288
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Auto Start
Group     = ShellSvcGroup

Name      = smphost
Display   = @%SystemRoot%\System32\smphost.dll,-102
ImagePath = %SystemRoot%\System32\svchost.exe -k smphost
Type      = Own_Process
Start     = Manual
Group     =

Name      = SmsRouter
Display   = @%SystemRoot%\System32\SmsRouterSvc.dll,-10001
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = SNMPTRAP
Display   = @%SystemRoot%\system32\snmptrap.exe,-3
ImagePath = %SystemRoot%\System32\snmptrap.exe
Type      = Own_Process
Start     = Manual
Group     =

Name      = Spooler
Display   = @%systemroot%\system32\spoolsv.exe,-1
ImagePath = %SystemRoot%\System32\spoolsv.exe
Type      = 0x0
Start     = Auto Start
Group     = SpoolerGroup

Name      = sppsvc
Display   = @%SystemRoot%\system32\sppsvc.exe,-101
ImagePath = %SystemRoot%\system32\sppsvc.exe
Type      = Own_Process
Start     = Auto Start
Group     =

Name      = srv
Display   = @%systemroot%\system32\srvsvc.dll,-102
ImagePath = System32\DRIVERS\srv.sys
Type      = File system driver
Start     = Auto Start
Group     = Network

Name      = srv2
Display   = @%systemroot%\system32\srvsvc.dll,-104
ImagePath = System32\DRIVERS\srv2.sys
Type      = File system driver
Start     = Manual
Group     = Network
```

Page 75

```
                            SYSTEM OUTPUT.txt
Name      = SSDPSRV
Display   = @%systemroot%\system32\ssdpsrv.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Manual
Group     =

Name      = SstpSvc
Display   = @%SystemRoot%\system32\sstpsvc.dll,-200
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService
Type      = Share_Process
Start     = Manual
Group     =

Name      = StateRepository
Display   = @%SystemRoot%\system32\windows.staterepository.dll,-1
ImagePath = %SystemRoot%\system32\svchost.exe -k appmodel
Type      = Share_Process
Start     = Manual
Group     =

Name      = storqosflt
Display   = @%SystemRoot%\System32\drivers\storqosflt.sys,-101
ImagePath = system32\drivers\storqosflt.sys
Type      = File system driver
Start     = Auto Start
Group     = FSFilter Quota Management

Name      = StorSvc
Display   = @%SystemRoot%\System32\StorSvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = svsvc
Display   = @%SystemRoot%\system32\svsvc.dll,-101
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = swprv
Display   = @%SystemRoot%\System32\swprv.dll,-103
ImagePath = %SystemRoot%\System32\svchost.exe -k swprv
Type      = Own_Process
Start     = Manual
Group     =

Name      = SysMain
Display   = @%SystemRoot%\system32\sysmain.dll,-1000
ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     =

Name      = SystemEventsBroker
Display   = @%windir%\system32\SystemEventsBrokerServer.dll,-1001
ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch
Type      = Share_Process
Start     = Auto Start
Group     =
```

Page 76

```
                              SYSTEM OUTPUT.txt
Name      = TapiSrv
Display   = @%SystemRoot%\system32\tapisrv.dll,-10100
ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService
Type      = Share_Process
Start     = Manual
Group     =

Name      = tcpipreg
Display   = TCP/IP Registry Compatibility
ImagePath = System32\drivers\tcpipreg.sys
Type      = Kernel driver
Start     = Auto Start
Group     =

Name      = tdx
Display   = @%SystemRoot%\system32\tcpipcfg.dll,-50004
ImagePath = \SystemRoot\system32\DRIVERS\tdx.sys
Type      = Kernel driver
Start     = System Start
Group     = PNP_TDI

Name      = TermService
Display   = @%SystemRoot%\System32\termsrv.dll,-268
ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService
Type      = Share_Process
Start     = Manual
Group     =

Name      = Themes
Display   = @%SystemRoot%\System32\themeservice.dll,-8192
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Auto Start
Group     = ProfSvc_Group

Name      = tiledatamodelsvc
Display   = @%SystemRoot%\system32\tileobjserver.dll,-1
ImagePath = %systemroot%\system32\svchost.exe -k appmodel
Type      = Share_Process
Start     = Auto Start
Group     =

Name      = TimeBroker
Display   = @%windir%\system32\TimeBrokerServer.dll,-1001
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Manual
Group     =

Name      = TrkWks
Display   = @%SystemRoot%\system32\trkwks.dll,-1
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     =

Name      = TsUsbFlt
Display   = @%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
ImagePath = System32\drivers\TsUsbFlt.sys
Type      = Kernel driver
Start     = Manual
Group     = base
```

Page 77

SYSTEM OUTPUT.txt

```
Name      = UcmCx0101
Display   = USB Connector Manager KMDF Class Extension
ImagePath = System32\Drivers\UcmCx.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Name      = UdeCx
Display   = USB Device Emulation Support Library
ImagePath = system32\drivers\udecx.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = udfs
Display   = udfs
ImagePath = system32\DRIVERS\udfs.sys
Type      = File system driver
Start     = Disabled
Group     = Boot File System

Name      = Ufx01000
Display   = USB Function Class Extension
ImagePath = system32\drivers\ufx01000.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Name      = UIODetect
Display   = @%SystemRoot%\system32\ui0detect.exe,-101
ImagePath = %SystemRoot%\system32\UIODetect.exe
Type      = 0x0
Start     = Manual
Group     =

Name      = UnistoreSvc
Display   = @%SystemRoot%\system32\UserDataAccessRes.dll,-10003
ImagePath = %SystemRoot%\System32\svchost.exe -k UnistackSvcGroup
Type      = 0x0
Start     = Manual
Group     =

Name      = upnphost
Display   = @%systemroot%\system32\upnphost.dll,-213
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Manual
Group     =

Name      = UrsCx01000
Display   = USB Role-Switch Support Library
ImagePath = system32\drivers\urscx01000.sys
Type      = Kernel driver
Start     = Manual
Group     = System Bus Extender

Name      = UserDataSvc
Display   = @%SystemRoot%\system32\UserDataAccessRes.dll,-14001
ImagePath = %SystemRoot%\system32\svchost.exe -k UnistackSvcGroup
Type      = 0x0
Start     = Manual
Group     =
```

Page 78

```
                              SYSTEM OUTPUT.txt
Name      = UserManager
Display   = @%systemroot%\system32\usermgr.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Auto Start
Group     =

Name      = UsoSvc
Display   = @%systemroot%\system32\usocore.dll,-102
ImagePath = %systemroot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = VaultSvc
Display   = @%SystemRoot%\system32\vaultsvc.dll,-1003
ImagePath = %SystemRoot%\system32\lsass.exe
Type      = Share_Process
Start     = Manual
Group     =

Name      = vds
Display   = @%SystemRoot%\system32\vds.exe,-100
ImagePath = %SystemRoot%\System32\vds.exe
Type      = Own_Process
Start     = Manual
Group     =

Name      = vhf
Display   = @%SystemRoot%\system32\drivers\vhf.sys,-100
ImagePath = \SystemRoot\System32\drivers\vhf.sys
Type      = Kernel driver
Start     = Manual
Group     = Base

Name      = vmicguestinterface
Display   = @%systemroot%\system32\icsvc.dll,-801
ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = vmicheartbeat
Display   = @%systemroot%\system32\icsvc.dll,-101
ImagePath = %systemroot%\system32\svchost.exe -k ICService
Type      = Share_Process
Start     = Manual
Group     =

Name      = vmickvpexchange
Display   = @%systemroot%\system32\icsvc.dll,-201
ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = vmicrdv
Display   = @%systemroot%\system32\icsvc.dll,-601
ImagePath = %systemroot%\system32\svchost.exe -k ICService
Type      = Share_Process
Start     = Manual
Group     =
```

Page 79

SYSTEM OUTPUT.txt
```
Name        = vmicshutdown
Display     = @%systemroot%\system32\icsvc.dll,-301
ImagePath   = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = vmictimesync
Display     = @%systemroot%\system32\icsvc.dll,-401
ImagePath   = %systemroot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = vmicvmsession
Display     = @%systemroot%\system32\icsvc.dll,-901
ImagePath   = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = vmicvss
Display     = @%systemroot%\system32\icsvc.dll,-501
ImagePath   = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = volmgrx
Display     = @%SystemRoot%\system32\drivers\volmgrx.sys,-100
ImagePath   = System32\drivers\volmgrx.sys
Type        = Kernel driver
Start       = Boot Start
Group       = System Bus Extender

Name        = VSS
Display     = @%systemroot%\system32\vssvc.exe,-102
ImagePath   = %systemroot%\system32\vssvc.exe
Type        = Own_Process
Start       = Manual
Group       =

Name        = W32Time
Display     = @%SystemRoot%\system32\w32time.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = WalletService
Display     = @%SystemRoot%\System32\WalletService.dll,-1000
ImagePath   = %SystemRoot%\System32\svchost.exe -k appmodel
Type        = Share_Process
Start       = Manual
Group       =

Name        = wbengine
Display     = @%systemroot%\system32\wbengine.exe,-104
ImagePath   = "%systemroot%\system32\wbengine.exe"
Type        = Own_Process
Start       = Manual
Group       =
```

Page 80

```
                         SYSTEM OUTPUT.txt
Name      = WbioSrvc
Display   = @%systemroot%\system32\wbiosrvc.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k WbioSvcGroup
Type      = Share_Process
Start     = Manual
Group     = SmartCardGroup

Name      = WCMSVC
Display   = @%SystemRoot%\System32\wcmsvc.dll,-4097
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     = TDI

Name      = wcncsvc
Display   = @%SystemRoot%\system32\wcncsvc.dll,-3
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceAndNoImpersonation
Type      = Share_Process
Start     = Manual
Group     =

Name      = WcsPlugInService
Display   = @%SystemRoot%\system32\WcsPlugInService.dll,-200
ImagePath = %SystemRoot%\system32\svchost.exe -k wcssvc
Type      = Share_Process
Start     = Manual
Group     =

Name      = WdiServiceHost
Display   = @%systemroot%\system32\wdi.dll,-502
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalService
Type      = Share_Process
Start     = Manual
Group     =

Name      = WdiSystemHost
Display   = @%systemroot%\system32\wdi.dll,-500
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = wdiwifi
Display   = WDI Driver Framework
ImagePath = system32\DRIVERS\wdiwifi.sys
Type      = Kernel driver
Start     = Manual
Group     =

Name      = WdNisSvc
Display   = @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-320
ImagePath = "%ProgramFiles%\Windows Defender\NisSrv.exe"
Type      = Own_Process
Start     = Manual
Group     =

Name      = WebClient
Display   = @%systemroot%\system32\webclnt.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService
Type      = Share_Process
Start     = Manual
Group     = NetworkProvider
```

Page 81

```
                    SYSTEM OUTPUT.txt
Name        = Wecsvc
Display     = @%SystemRoot%\system32\wecsvc.dll,-200
ImagePath   = %SystemRoot%\system32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =

Name        = WEPHOSTSVC
Display     = @%systemroot%\system32\wephostsvc.dll,-100
ImagePath   = %systemroot%\system32\svchost.exe -k WepHostSvcGroup
Type        = Share_Process
Start       = Manual
Group       =

Name        = wercplsupport
Display     = @%SystemRoot%\System32\wercplsupport.dll,-101
ImagePath   = %SystemRoot%\System32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = WerSvc
Display     = @%SystemRoot%\System32\wersvc.dll,-100
ImagePath   = %SystemRoot%\System32\svchost.exe -k WerSvcGroup
Type        = Own_Process
Start       = Manual
Group       =

Name        = WiaRpc
Display     = @%SystemRoot%\system32\wiarpc.dll,-2
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = WIMMount
Display     = WIMMount
ImagePath   = system32\drivers\wimmount.sys
Type        = File system driver
Start       = Manual
Group       = FSFilter Infrastructure

Name        = WinHttpAutoProxySvc
Display     = @%SystemRoot%\system32\winhttp.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       =

Name        = Winmgmt
Display     = @%Systemroot%\system32\wbem\wmisvc.dll,-205
ImagePath   = %systemroot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Auto Start
Group       =

Name        = WinRM
Display     = @%Systemroot%\system32\wsmsvc.dll,-101
ImagePath   = %SystemRoot%\System32\svchost.exe -k NetworkService
Type        = Share_Process
Start       = Manual
Group       =
```

Page 82

```
                        SYSTEM OUTPUT.txt
Name        = wlidsvc
Display     = @%SystemRoot%\system32\wlidsvc.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k netsvcs
Type        = Share_Process
Start       = Manual
Group       =

Name        = wmiApSrv
Display     = @%Systemroot%\system32\wbem\wmiapsrv.exe,-110
ImagePath   = %systemroot%\system32\wbem\WmiApSrv.exe
Type        = Own_Process
Start       = Manual
Group       =

Name        = WMPNetworkSvc
Display     = @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101
ImagePath   = "%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe"
Type        = Own_Process
Start       = Manual
Group       =

Name        = Wof
Display     = Windows Overlay File System Filter Driver
ImagePath   =
Type        = File system driver
Start       = Boot Start
Group       = FSFilter Compression

Name        = workfolderssvc
Display     = @%systemroot%\system32\workfolderssvc.dll,-102
ImagePath   = %SystemRoot%\System32\svchost.exe -k LocalService
Type        = Share_Process
Start       = Manual
Group       = LocalService

Name        = wpcfltr
Display     = Family Safety Filter Driver
ImagePath   = system32\DRIVERS\wpcfltr.sys
Type        = Kernel driver
Start       = Manual
Group       = NDIS

Name        = WPDBusEnum
Display     = @%SystemRoot%\system32\wpdbusenum.dll,-100
ImagePath   = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type        = Share_Process
Start       = Manual
Group       =

Name        = WpnService
Display     = @%SystemRoot%\system32\wpnservice.dll,-1
ImagePath   = %systemroot%\system32\svchost.exe -k wswpnservice
Type        = Share_Process
Start       = Manual
Group       =

Name        = ws2ifsl
Display     = @%systemroot%\System32\drivers\ws2ifsl.sys,-1000
ImagePath   = \SystemRoot\system32\drivers\ws2ifsl.sys
Type        = Kernel driver
Start       = Disabled
Group       = PNP_TDI
```

Page 83

SYSTEM OUTPUT.txt

```
Name      = wscsvc
Display   = @%SystemRoot%\System32\wscsvc.dll,-200
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type      = Share_Process
Start     = Auto Start
Group     =

Name      = WSService
Display   = @%SystemRoot%\system32\WSService.dll,-103
ImagePath = %SystemRoot%\System32\svchost.exe -k wsappx
Type      = Share_Process
Start     = Manual
Group     =

Name      = WudfPf
Display   = @%SystemRoot%\system32\drivers\Wudfpf.sys,-1000
ImagePath = system32\drivers\WudfPf.sys
Type      = Kernel driver
Start     = Manual
Group     = base

Name      = wudfsvc
Display   = @%SystemRoot%\system32\wudfsvc.dll,-1000
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     = PlugPlay

Name      = WwanSvc
Display   = @%SystemRoot%\System32\wwansvc.dll,-257
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork
Type      = Share_Process
Start     = Manual
Group     = TDI

Name      = XblAuthManager
Display   = @%systemroot%\system32\XblAuthManager.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = XblGameSave
Display   = @%systemroot%\system32\XblGameSave.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = XboxNetApiSvc
Display   = @%systemroot%\system32\XboxNetApiSvc.dll,-100
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Fri Jul 10 11:05:06 2015Z
Name      = .NET CLR Networking 4.0.0.0
Display   =
ImagePath =
Type      =
Start     =
Group     =
```

Page 84

SYSTEM OUTPUT.txt

```
Name       = .NET Data Provider for Oracle
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = .NET Data Provider for SqlServer
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = .NET Memory Cache 4.0
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = .NETFramework
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = ADOVMPPackage
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = adsi
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = BattC
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = clr_optimization_v4.0.30319_32
Display    =
ImagePath  =
Type       =
Start      =
Group      =

Name       = clr_optimization_v4.0.30319_64
Display    =
ImagePath  =
Type       =
Start      =
Group      =
```

Page 85

SYSTEM OUTPUT.txt

```
Name        = CoreUI
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = DCLocator
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = ESENT
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Fri Jul 10 11:05:05 2015Z
Name        = inetaccs
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = ldap
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = Lsa
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = Msfs
Display     =
ImagePath   =
Type        = File system driver
Start       = System Start
Group       = File system

Name        = MSRPC
Display     =
ImagePath   =
Type        = Kernel driver
Start       = Manual
Group       =

Name        = MSSCNTRS
Display     =
ImagePath   =
Type        =
Start       =
```

Page 86

SYSTEM OUTPUT.txt

```
Group       =

Name        = napagent
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = Npfs
Display     =
ImagePath   =
Type        = File system driver
Start       = System Start
Group       = File system

Name        = NTDS
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = Null
Display     =
ImagePath   =
Type        = Kernel driver
Start       = System Start
Group       = Base

Name        = PerfDisk
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = PerfNet
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = PerfOS
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = PerfProc
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = PortProxy
Display     =
ImagePath   =
Type        =
Start       =
```

Page 87

SYSTEM OUTPUT.txt

```
Group       =

Name        = RasAcd
Display     = Remote Access Auto Connection Driver
ImagePath   = System32\DRIVERS\rasacd.sys
Type        = Kernel driver
Start       = Manual
Group       = Streams Drivers

Name        = RDPNP
Display     = @%systemroot%\system32\drprov.dll,-100
ImagePath   =
Type        =
Start       =
Group       =

Name        = TSDDD
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = UGatherer
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = UGTHRSVC
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = VerifierExt
Display     = @%SystemRoot%\system32\drivers\VerifierExt.sys,-1000
ImagePath   = system32\drivers\VerifierExt.sys
Type        = Kernel driver
Start       = Manual
Group       = WdfLoadGroup

Name        = WinSock2
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = WmiApRpl
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = workerdd
Display     =
ImagePath   =
Type        =
Start       =
```

Page 88

SYSTEM OUTPUT.txt

```
Group       =

Name        = WSearchIdxPi
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Name        = xmlprov
Display     =
ImagePath   =
Type        =
Start       =
Group       =

Fri Jul 10 11:04:15 2015z
    Name        = TsUsbGD
    Display     = @tsgenericusbdriver.inf,%TsUsbGD.DeviceDesc.Generic%
    ImagePath   = Remote Desktop Generic USB Device
    Type        = \SystemRoot\System32\drivers\TsUsbGD.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = UrsChipidea
    Display     = @urschipidea.inf,%UrsChipidea.ServiceName%
    ImagePath   = Chipidea USB Role-Switch Driver
    Type        = \SystemRoot\System32\drivers\urschipidea.sys
    Start       = Kernel driver
    Group       = Manual;Base

    Name        = UrsSynopsys
    Display     = @urssynopsys.inf,%UrsSynopsys.ServiceName%
    ImagePath   = Synopsys USB Role-Switch Driver
    Type        = \SystemRoot\System32\drivers\urssynopsys.sys
    Start       = Kernel driver
    Group       = Manual;Base

Fri Jul 10 11:04:13 2015z
    Name        = vhdmp
    Display     =
    ImagePath   = \SystemRoot\System32\drivers\vhdmp.sys
    Type        = Kernel driver
    Start       = Manual
    Group       = SCSI miniport

Fri Jul 10 11:04:12 2015z
    Name        = AmdK8
    Display     = @cpu.inf,%AmdK8.SvcDesc%
    ImagePath   = AMD K8 Processor Driver
    Type        = \SystemRoot\System32\drivers\amdk8.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = AmdPPM
    Display     = @cpu.inf,%AmdPPM.SvcDesc%
    ImagePath   = AMD Processor Driver
    Type        = \SystemRoot\System32\drivers\amdppm.sys
    Start       = Kernel driver
    Group       = Manual;Extended Base

    Name        = Processor
    Display     = @cpu.inf,%Processor.SvcDesc%
```

Page 89

SYSTEM OUTPUT.txt
```
ImagePath = Processor Driver
Type      = \SystemRoot\System32\drivers\processr.sys
Start     = Kernel driver
Group     = Manual;Extended Base

Fri Jul 10 11:04:11 2015Z
Name      = UfxChipidea
Display   = @ufxchipidea.inf,%UfxChipidea.ServiceName%
ImagePath = USB Chipidea Controller
Type      = \SystemRoot\System32\drivers\UfxChipidea.sys
Start     = Kernel driver
Group     = Manual;Base

Name      = ufxsynopsys
Display   = @ufxsynopsys.inf,%ufxsynopsys.ServiceName%
ImagePath = USB Synopsys Controller
Type      = \SystemRoot\System32\drivers\ufxsynopsys.sys
Start     = Kernel driver
Group     = Manual;Base

Fri Jul 10 11:04:08 2015Z
Name      = ibbus
Display   = @mlx4_bus.inf,%Ibbus.ServiceDesc%
ImagePath = Mellanox InfiniBand Bus/AL (Filter Driver)
Type      = \SystemRoot\System32\drivers\ibbus.sys
Start     = Kernel driver
Group     = Manual;PnP Filter

Name      = mlx4_bus
Display   = @mlx4_bus.inf,%MLX4BUS.ServiceDesc%
ImagePath = Mellanox ConnectX Bus Enumerator
Type      = \SystemRoot\System32\drivers\mlx4_bus.sys
Start     = Kernel driver
Group     = Manual;NDIS

Name      = ndfltr
Display   = @mlx4_bus.inf,%ndfltr.ServiceDesc%
ImagePath = NetworkDirect Service
Type      = \SystemRoot\System32\drivers\ndfltr.sys
Start     = Kernel driver
Group     = Manual;PNP Filter

Name      = sermouse
Display   = @msmouse.inf,%sermouse.SvcDesc%
ImagePath = Serial Mouse Driver
Type      = \SystemRoot\System32\drivers\sermouse.sys
Start     = Kernel driver
Group     = Manual;Pointer Port

Name      = WinMad
Display   = @mlx4_bus.inf,%WinMad.ServiceDesc%
ImagePath = WinMad Service
Type      = \SystemRoot\System32\drivers\winmad.sys
Start     = Kernel driver
Group     = Manual;PNP Filter

Name      = WinVerbs
Display   = @mlx4_bus.inf,%WinVerbs.ServiceDesc%
ImagePath = WinVerbs Service
Type      = \SystemRoot\System32\drivers\winverbs.sys
Start     = Kernel driver
Group     = Manual;PNP Filter
```

Page 90

```
                          SYSTEM OUTPUT.txt
Fri Jul 10 11:04:04 2015Z
    Name       = hidinterrupt
    Display    = @hidinterrupt.inf,%HID.SvcDesc%
    ImagePath  = Common Driver for HID Buttons implemented with interrupts
    Type       = \SystemRoot\System32\drivers\hidinterrupt.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = WacomPen
    Display    = @hiddigi.inf,%WacomPen.SVCDESC%
    ImagePath  = Wacom Serial Pen HID Driver
    Type       = \SystemRoot\System32\drivers\wacompen.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

Fri Jul 10 11:04:03 2015Z
    Name       = acpitime
    Display    = @acpitime.inf,%AcpiTime.SvcDesc%
    ImagePath  = ACPI Wake Alarm Driver
    Type       = \SystemRoot\System32\drivers\acpitime.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = bcmfn2
    Display    = @bcmfn2.inf,%bcmfn2.SVCDESC%
    ImagePath  = bcmfn2 Service
    Type       = \SystemRoot\System32\drivers\bcmfn2.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = ErrDev
    Display    = @errdev.inf,%ERRDEV.SvcDesc%
    ImagePath  = Microsoft Hardware Error Device Driver
    Type       = \SystemRoot\System32\drivers\errdev.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = genericusbfn
    Display    = @genericusbfn.inf,%genericusbfn.ServiceName%
    ImagePath  = Generic USB Function Class
    Type       = \SystemRoot\System32\drivers\genericusbfn.sys
    Start      = Kernel driver
    Group      = Manual;Base

Fri Jul 10 11:04:01 2015Z
    Name       = wfpcapture
    Display    = @wfpcapture.inf,%WfpCapture_Desc%
    ImagePath  = Microsoft WFP Message Capture
    Type       = \SystemRoot\System32\drivers\wfpcapture.sys
    Start      = Kernel driver
    Group      = Manual;NDIS

    Name       = xinputhid
    Display    = @xinputhid.inf,%xinputhid.SvcDesc%
    ImagePath  = XINPUT HID Filter Driver
    Type       = \SystemRoot\System32\drivers\xinputhid.sys
    Start      = Kernel driver
    Group      = Manual;Base

Fri Jul 10 11:04:00 2015Z
    Name       = usbcir
    Display    = @usbcir.inf,%usbcir.SVCDESC%
    ImagePath  = eHome Infrared Receiver (USBCIR)
                                                  Page 91
```

```
                              SYSTEM OUTPUT.txt
    Type       = \SystemRoot\System32\drivers\usbcir.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

Fri Jul 10 11:03:59 2015Z
    Name       = circlass
    Display    = @circlass.inf,%circlass.SVCDESC%
    ImagePath  = Consumer IR Devices
    Type       = \SystemRoot\System32\drivers\circlass.sys
    Start      = Kernel driver
    Group      = Manual;Extended Base

    Name       = HidBth
    Display    = @hidbth.inf,%HIDBTH.SvcDesc%
    ImagePath  = Microsoft Bluetooth HID Miniport
    Type       = \SystemRoot\System32\drivers\hidbth.sys
    Start      = Kernel driver
    Group      = Manual;extended base

    Name       = HidIr
    Display    = @hidir.inf,%HIDIR.SvcDesc%
    ImagePath  = Microsoft Infrared HID Driver
    Type       = \SystemRoot\System32\drivers\hidir.sys
    Start      = Kernel driver
    Group      = Manual;extended base

Fri Jul 10 11:03:58 2015Z
    Name       = fcvsc
    Display    =
    ImagePath  = \SystemRoot\System32\drivers\fcvsc.sys
    Type       = Kernel driver
    Start      = Manual
    Group      = SCSI miniport

    Name       = vpci
    Display    = @wvpci.inf,%vpci.SVCDESC%
    ImagePath  = Microsoft Hyper-V Virtual PCI Bus
    Type       = \SystemRoot\System32\drivers\vpci.sys
    Start      = Kernel driver
    Group      = Manual;System Bus Extender

-------------------------------------------
shares v.20140730
(System) Get list of shares from System hive file

 subkey not found.
-------------------------------------------
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Thu Apr 21 04:41:23 2016 (UTC)
   ShutdownTime = Thu Apr 21 04:41:23 2016 (UTC)
-------------------------------------------
shutdowncount v.20080709
(System) Retrieves ShutDownCount value

ControlSet001\Control\Watchdog\Display not found.
-------------------------------------------
stillimage v.20100222
(System) Get info on StillImage devices
```

Page 92

SYSTEM OUTPUT.txt

StillImage Logging Level
  STICLI Logging Level = 0x4
  STIMON Logging Level = 0x4
-----------------------------------------------
svc v.20131010
(System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName
Thu Apr 21 04:41:25 2016 Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,Kernel driver,Manual,,McAfee Proxy Service
Thu Apr 21 04:41:19 2016 Z,mfemms,McAfee Service Controller,"C:\Program Files\Common
Files\McAfee\SystemCore\\mfemms.exe",Own_Process,Auto Start,LocalSystem,Manages
McAfee Services
Thu Apr 21 04:41:16 2016 Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,,McAfee Proxy Service
Thu Apr 21 04:41:15 2016 Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor
Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",Own_Process,Auto
Start,LocalSystem,McAfee SiteAdvisor Service
Thu Apr 21 04:41:15 2016 Z,McAPExe,McAfee AP Service,"C:\Program
Files\McAfee\MSC\McAPExe.exe",Own_Process,Auto Start,LocalSystem,McAfee AP Service
Thu Apr 21 04:41:15 2016 Z,McMPFSvc,McAfee Personal Firewall Service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem,Helps protect your computer from
intrusion and let's you manage your computer's trusted programs.
Thu Apr 21 04:41:15 2016 Z,McProxy,McAfee Proxy Service,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto
Start,LocalSystem,McAfee Proxy Service
Thu Apr 21 04:41:15 2016
Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,,
Thu Apr 21 03:24:59 2016
Z,MBAMSwissArmy,MBAMSwissArmy,\??\C:\Windows\system32\drivers\MBAMSwissArmy.sys,File
system driver,Manual,,Malwarebytes Anti-Malware service
Thu Apr 21 03:20:08 2016 Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,,Provides firewall
services to McAfee products
Thu Apr 21 03:19:52 2016 Z,cfwids,McAfee Inc.
cfwids,system32\drivers\cfwids.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\certprop.dll,-12
Thu Apr 21 03:19:50 2016 Z,mfencbdc,McAfee Inc.
mfencbdc,\SystemRoot\system32\DRIVERS\mfencbdc.sys,Kernel driver,Manual,,McAfee
Content driver Copyright (C) 2015 McAfee, Inc. All Rights Reserved.
Thu Apr 21 03:19:31 2016 Z,UmPass,@umpass.inf;%UmPass.SVCDESC%;Microsoft UMPass
Driver,\SystemRoot\System32\drivers\umpass.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102
Thu Apr 21 03:19:16 2016 Z,tunnel,@nettun.inf;%TUNNEL.Service.DisplayName%;Microsoft
Tunnel Miniport Adapter Driver,\SystemRoot\System32\drivers\tunnel.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Thu Apr 21 03:19:15 2016
Z,vwifimp,@%SystemRoot%\System32\drivers\vwifimp.sys;-261,\SystemRoot\System32\drive
rs\vwifimp.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\vwififlt.sys,-260
Thu Apr 21 03:19:03 2016
Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,,
Thu Apr 21 03:18:58 2016
Z,BasicDisplay,,\SystemRoot\System32\drivers\BasicDisplay.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\AxInstSV.dll,-104
Thu Apr 21 03:18:58 2016 Z,monitor,@monitor.inf;%Monitor.SVCDESC%;Microsoft Monitor
Class Function Driver Service,\SystemRoot\System32\drivers\monitor.sys,Kernel
driver,Manual,,McAfee Module Core Service
Thu Apr 21 03:18:57 2016
Z,BtFilter,BtFilter,\SystemRoot\system32\DRIVERS\btfilter.sys,Kernel

Page 93

SYSTEM OUTPUT.txt

driver,Manual,,@%systemroot%\system32\browser.dll,-101
Thu Apr 21 03:18:57 2016 Z,BTHUSB,@bth.inf;%BTHUSB.SvcDesc%;Bluetooth Radio USB
Driver,\SystemRoot\System32\Drivers\BTHUSB.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102
Thu Apr 21 03:18:57 2016 Z,RTSUER,@oem14.inf;%RtsUER%;Realtek USB Card Reader -
UER,\SystemRoot\system32\Drivers\RtsUer.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ltdres.dll,-5
Thu Apr 21 03:18:56 2016 Z,HidUsb,@input.inf;%HID.SvcDesc%;Microsoft HID Class
Driver,\SystemRoot\System32\drivers\hidusb.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\hidserv.dll,-102
Thu Apr 21 03:18:56 2016 Z,usbccgp,@usb.inf;%GenericParent.SvcDesc%;Microsoft USB
Generic Parent Driver,\SystemRoot\System32\drivers\usbccgp.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Thu Apr 21 03:18:56 2016 Z,usbvideo,@usbvideo.inf;%USBVideo.SvcDesc%;USB Video
Device (WDM),\SystemRoot\System32\Drivers\usbvideo.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Thu Apr 21 03:18:55 2016 Z,ETDI2C,@oem13.inf;%ELANI2CDeviceDesc%;ELAN I2C Filter
Driver,\SystemRoot\system32\DRIVERS\ETDI2C.sys,Kernel driver,Manual,,ePower Service
Thu Apr 21 03:18:55 2016 Z,hidi2c,@hidi2c.inf;%hidi2c.SVCDESC%;Microsoft I2C HID
Miniport Driver,\SystemRoot\System32\drivers\hidi2c.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Thu Apr 21 03:18:55 2016 Z,IntcDAud,@oem6.inf;%IntcDAud.SvcDesc%;Intel(R) Display
Audio,\SystemRoot\system32\DRIVERS\IntcDAud.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Thu Apr 21 03:18:55 2016 Z,mouclass,@msmouse.inf;%mouclass.SvcDesc%;Mouse Class
Driver,\SystemRoot\System32\drivers\mouclass.sys,Kernel driver,Manual,,McAfee Module
Core Service
Thu Apr 21 03:18:55 2016 Z,mouhid,@msmouse.inf;%MOUHID.SvcDesc%;Mouse HID
Driver,\SystemRoot\System32\drivers\mouhid.sys,Kernel driver,Manual,,McAfee Module
Core Service
Thu Apr 21 03:18:55 2016
Z,mshidkmdf,,\SystemRoot\System32\drivers\mshidkmdf.sys,Kernel
driver,Manual,,@comres.dll,-2798
Thu Apr 21 03:18:55 2016 Z,MTConfig,@mtconfig.inf;%MTConfig.SVCDESC%;Microsoft Input
Configuration Driver,\SystemRoot\System32\drivers\MTConfig.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Thu Apr 21 03:18:54 2016 Z,IntcAzAudAddService,service for Realtek HD Audio
(WDM),\SystemRoot\system32\drivers\RTKVHD64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Thunks,\SystemRoot\system32\ksthunk,Kernel Streaming
driver,Manual,,@keyiso.dll,-101
Thu Apr 21 03:18:54 2016 Z,USBHUB3,@usbhub3.inf;%UsbHub3.SVCDESC%;SuperSpeed
Hub,\SystemRoot\System32\drivers\UsbHub3.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Thu Apr 21 03:18:51 2016 Z,mssmbios,@mssmbios.inf;%mssmbios_svcdesc%;Microsoft
System Management BIOS Driver,\SystemRoot\System32\drivers\mssmbios.sys,Kernel
driver,System Start,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Thu Apr 21 03:18:49 2016 Z,ACPI,@acpi.inf;%ACPI.SvcDesc%;Microsoft ACPI
Driver,System32\drivers\ACPI.sys,Kernel driver,Boot Start,;
Thu Apr 21 03:18:49 2016 Z,athr,@oem10.inf;%ATHR.Service.DispName%;Qualcomm Atheros
Extensible Wireless LAN device
driver,\SystemRoot\System32\drivers\athw10x.sys,Kernel driver,Manual,,Atheros BT
Stack Service Agent
Thu Apr 21 03:18:49 2016 Z,cdrom,@cdrom.inf;%cdrom_ServiceDesc%;CD-ROM
Driver,\SystemRoot\System32\drivers\cdrom.sys,Kernel driver,System
start,,@%SystemRoot%\system32\cdpsvc.dll,-101
Thu Apr 21 03:18:49 2016 Z,CmBatt,@cmbatt.inf;%CmBatt.SvcDesc%;Microsoft ACPI
Control Method Battery Driver,\SystemRoot\System32\drivers\CmBatt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ClipSVC.dll,-104
Thu Apr 21 03:18:49 2016 Z,disk,@disk.inf;%disk_serviceDesc%;Disk
Driver,System32\drivers\disk.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\diagtrack.dll,-3002

Page 94

SYSTEM OUTPUT.txt

Thu Apr 21 03:18:49 2016
Z,EhStorClass,@%SystemRoot%\system32\drivers\EhStorClass.sys;-100,System32\drivers\E
hStorClass.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\EhStorClass.sys,-101
Thu Apr 21 03:18:49 2016
Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.sys,
Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\fvevol.sys,-100
Thu Apr 21 03:18:49 2016 Z,GPIO,@oem4.inf;%GPIO.SVCDESC%;Intel SoC GPIO Controller
Driver,\SystemRoot\System32\drivers\iaiogpioe.sys,Kernel driver,Manual,,WT Games App
Services
Thu Apr 21 03:18:49 2016 Z,HDAudBus,@hdaudbus.inf;%HDAudBus.SVCDESC%;Microsoft UAA
Bus Driver for High Definition
Audio,\SystemRoot\System32\drivers\HDAudBus.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Thu Apr 21 03:18:49 2016 Z,i8042prt,@keyboard.inf;%i8042prt.SvcDesc%;i8042 Keyboard
and PS/2 Mouse Port Driver,\SystemRoot\System32\drivers\i8042prt.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Apr 21 03:18:49 2016 Z,iaioi2c,@oem5.inf;%Driver_Service.Desc%;I2C Controller
Service,\SystemRoot\System32\drivers\iaioi2ce.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Apr 21 03:18:49 2016 Z,igfx,,\SystemRoot\system32\DRIVERS\igdkmd64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001
Thu Apr 21 03:18:49 2016 Z,intelpep,@intelpep.inf;%INTELPEP.SVCDESC%;Intel(R) Power
Engine Plug-in Driver,System32\drivers\intelpep.sys,Kernel driver,Boot
Start,,Version: 1.35.117.1
Thu Apr 21 03:18:49 2016 Z,intelppm,@cpu.inf;%IntelPPM.SvcDesc%;Intel Processor
Driver,\SystemRoot\System32\drivers\intelppm.sys,Kernel driver,Manual,,Version:
1.35.117.1
Thu Apr 21 03:18:49 2016 Z,kbdclass,@keyboard.inf;%kbdclass.SvcDesc%;Keyboard Class
Driver,\SystemRoot\System32\drivers\kbdclass.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Thu Apr 21 03:18:49 2016 Z,mfewfpk,McAfee Inc.
mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,,Provides validation
trust protection services
Thu Apr 21 03:18:49 2016 Z,msisadrv,,System32\drivers\msisadrv.sys,Kernel
driver,Boot Start,,@comres.dll,-2798
Thu Apr 21 03:18:49 2016
Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partmgr.s
ys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\partmgr.sys,-101
Thu Apr 21 03:18:49 2016 Z,pci,@pci.inf;%pci_svcdesc%;PCI Bus
Driver,System32\drivers\pci.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Thu Apr 21 03:18:49 2016 Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel
driver,Boot Start,,ReadyBoost
Thu Apr 21 03:18:49 2016 Z,rt640x64,@oem12.inf;%rt640.Service.DispName%;Realtek
RT640 NT Driver,\SystemRoot\System32\drivers\rt640x64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lltdres.dll,-5
Thu Apr 21 03:18:49 2016
Z,storahci,@mshdc.inf;%storahci_ServiceDescription%;Microsoft Standard SATA AHCI
Driver,System32\drivers\storahci.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\wiaservc.dll,-10
Thu Apr 21 03:18:49 2016 Z,TXEIx64,@oem2.inf;%TEE_SvcDesc%;Intel(R) Trusted
Execution Engine Interface ,\SystemRoot\System32\drivers\TXEIx64.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Thu Apr 21 03:18:49 2016 Z,UEFI,@uefi.inf;%UEFI.SvcDesc%;Microsoft UEFI
Driver,\SystemRoot\System32\drivers\UEFI.sys,Kernel driver,Manual,,Reads/Writes UDF
1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)
Thu Apr 21 03:18:49 2016 Z,USBXHCI,@usbxhci.inf;%PCI\CC_0C0330.DeviceDesc%;USB xHCI
Compliant Host Controller,\SystemRoot\System32\drivers\USBXHCI.SYS,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Thu Apr 21 03:18:49 2016 Z,volsnap,@volume.inf;%VolumeClassName%;Storage
volumes,System32\drivers\volsnap.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101

Page 95

SYSTEM OUTPUT.txt

Thu Apr 21 03:18:49 2016
Z,vwifibus,@%SystemRoot%\System32\drivers\vwifibus.sys;-257,\SystemRoot\System32\dri
vers\vwifibus.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\vwifibus.sys,-258
Thu Apr 21 03:18:49 2016
Z,Wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wdf010
00.sys,Kernel driver,Boot Start,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-400
Thu Apr 21 03:18:49 2016 Z,WmiAcpi,@wmiacpi.inf;%WMIMAP.SvcDesc%;Microsoft Windows
Management Interface for ACPI,\SystemRoot\System32\drivers\wmiacpi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\wlidsvc.dll,-101
Thu Apr 21 03:18:48 2016
Z,BasicRender,,\SystemRoot\System32\drivers\BasicRender.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\AxInstSV.dll,-104
Thu Apr 21 03:18:48 2016
Z,CompositeBus,@compositebus.inf;%CompositeBus.SVCDESC%;Composite Bus Enumerator
Driver,\SystemRoot\System32\DriverStore\FileRepository\compositebus.inf_amd64_98334b
a6e76853ba\CompositeBus.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\cnghwassist.sys,-100
Thu Apr 21 03:18:48 2016 Z,iwdbus,@oem9.inf;%iwdbus.SVCDESC%;IWD Bus
Enumerator,\SystemRoot\System32\drivers\iwdbus.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Thu Apr 21 03:18:48 2016 Z,kdnic,@kdnic.inf;%KdNic.Service.DispName%;Microsoft
Kernel Debug Network Miniport (NDIS
6.20),\SystemRoot\System32\drivers\kdnic.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Thu Apr 21 03:18:48 2016 Z,LMDriver,@oem16.inf;%LMDriver.SVCDESC%;Launch Manager
Wireless Driver,\SystemRoot\System32\drivers\LMDriver.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lltdres.dll,-2
Thu Apr 21 03:18:48 2016
Z,NdisVirtualBus,@%SystemRoot%\System32\drivers\NdisVirtualBus.sys;-200,\SystemRoot\
System32\drivers\NdisVirtualBus.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001
Thu Apr 21 03:18:48 2016 Z,RadioShim,@oem16.inf;%RadioShim.SVCDESC%;Shim for
HID-KMDF Interface layer,\SystemRoot\System32\drivers\RadioShim.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\qwavedrv.sys,-2
Thu Apr 21 03:18:48 2016 Z,rdpbus,@rdpbus.inf;%rdpbus_svcdesc%;Remote Desktop Device
Redirector Bus Driver,\SystemRoot\System32\drivers\rdpbus.sys,Kernel
driver,Manual,,@%systemroot%\system32\wksvc.dll,-1001
Thu Apr 21 03:18:48 2016 Z,spaceport,@spaceport.inf;%Spaceport_ServiceDesc%;Storage
Spaces Driver,System32\drivers\spaceport.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\snmptrap.exe,-4
Thu Apr 21 03:18:48 2016 Z,swenum,@swenum.inf;%SWENUM.SVCDESC%;Software Bus
Driver,\SystemRoot\System32\DriverStore\FileRepository\swenum.inf_amd64_2a699e44676b
7781\swenum.sys,Kernel driver,Manual,,@%SystemRoot%\system32\svsvc.dll,-102
Thu Apr 21 03:18:48 2016 Z,tap0901,@oem23.inf;%DeviceDescription%;TAP-Windows
Adapter V9,\SystemRoot\System32\drivers\tap0901.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\TabSvc.dll,-101
Thu Apr 21 03:18:48 2016 Z,umbus,@umbus.inf;%umbus.SVCDESC%;UMBus Enumerator
Driver,\SystemRoot\System32\drivers\umbus.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\uiOdetect.exe,-102
Thu Apr 21 03:18:48 2016 Z,vdrvroot,@vdrvroot.inf;%vdrvroot_svcdesc%;Microsoft
Virtual Drive Enumerator,System32\drivers\vdrvroot.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\vaultsvc.dll,-1004
Thu Apr 21 03:18:48 2016 Z,volmgr,@volmgr.inf;%volmgr_svcdesc%;Volume Manager
Driver,System32\drivers\volmgr.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\icsvc.dll,-502
Thu Apr 21 03:15:49 2016 Z,mfesapsn,McAfee Process Start Notification
Service,\??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,Kernel
driver,Manual,,McAfee Content driver Copyright (C) 2015 McAfee, Inc. All Rights
Reserved.
Thu Apr 21 03:15:18 2016 Z,McPvDrv,McPvDrv
Driver,\SystemRoot\system32\drivers\McPvDrv.sys,Kernel driver,Auto Start,,McAfee
Proxy Service

Page 96

SYSTEM OUTPUT.txt
Thu Apr 21 03:15:06 2016 Z,MSK80Service,McAfee Anti-Spam Service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem,This service filters e-mail messages
on your computer
Thu Apr 21 03:14:14 2016 Z,HipShieldK,McAfee Inc.
HipShieldK,system32\drivers\HipShieldK.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\hidserv.dll,-102
Thu Apr 21 03:13:53 2016 Z,WdBoot,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-390,\SystemRoot\system32\drivers\WdBoot.sys,Kernel
driver,Manual,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-400
Thu Apr 21 03:13:53 2016 Z,WdFilter,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-330,\SystemRoot\system32\drivers\WdFilter.sys,File system
driver,Manual,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-340
Thu Apr 21 03:13:47 2016 Z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,Kernel driver,Boot Start,,Provides firewall
services to McAfee products
Thu Apr 21 03:13:47 2016 Z,WinDefend,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-310,"%ProgramFiles%\Windows
Defender\MsMpEng.exe",Own_Process,Manual,LocalSystem,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll,-240
Thu Apr 21 03:13:46 2016 Z,WdNisDrv,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-370,system32\Drivers\WdNisDrv.sys,Kernel
driver,Manual,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-242
Thu Apr 21 03:13:35 2016 Z,McODS,McAfee Scanner,"C:\Program
Files\McAfee\VirusScan\mcods.exe",Own_Process,Manual,LocalSystem,McAfee Scanner
Thu Apr 21 03:13:25 2016 Z,McNaiAnn,McAfee VirusScan Announcer,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee VirusScan Announcer
Thu Apr 21 03:12:49 2016 Z,mfencrk,McAfee Inc.
mfencrk,\SystemRoot\system32\DRIVERS\mfencrk.sys,Kernel driver,Manual,,McAfee
Content driver Copyright (C) 2015 McAfee, Inc. All Rights Reserved.
Thu Apr 21 03:12:03 2016 Z,McBootDelayStartSvc,McAfee Boot Delay Start
Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee Boot Delay Start Service
Thu Apr 21 03:12:02 2016 Z,mcpltsvc,McAfee Platform Services,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee Platform Services
Thu Apr 21 03:11:46 2016 Z,PEFService,Intel Security PEF Service,"C:\Program
Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",Own_Process,Auto
Start,LocalSystem,Intel Security PEF Service
Thu Apr 21 03:11:37 2016 Z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common
Files\McAfee\CSP\1.9.656.0\McCSPServiceHost.exe",Own_Process,Auto
Start,LocalSystem,McAfee Cloud Platform Service
Thu Apr 21 03:10:59 2016 Z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto
Start,LocalSystem,McAfee Home Network
Thu Apr 21 03:10:58 2016 Z,mfefire,McAfee Firewall Core Service,"C:\Program
Files\Common
Files\McAfee\SystemCore\\mfefire.exe",Own_Process,Manual,LocalSystem,Provides
firewall services to McAfee products
Thu Apr 21 03:10:57 2016 Z,mfevtp,McAfee Validation Trust Protection
Service,"C:\Windows\system32\mfevtps.exe",Own_Process,Manual,LocalSystem,Provides
validation trust protection services
Thu Apr 21 03:10:48 2016 Z,mfeelamk,McAfee Inc.
mfeelamk,system32\drivers\mfeelamk.sys,Kernel driver,Boot Start,,McAfee Proxy
Service
Thu Apr 21 03:08:54 2016 Z,ModuleCoreService,McAfee Module Core Service,"C:\Program
Files\Common Files\McAfee\ModuleCore\ModuleCoreService.exe",Share_Process,Auto
Start,LocalSystem,McAfee Module Core Service
Thu Apr 21 03:00:51 2016
Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\qmgr.dll,-1001
Sun Apr 17 00:48:02 2016

Page 97

SYSTEM OUTPUT.txt
Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\se
rvicing\TrustedInstaller.exe,Own_Process,Manual,localSystem,@%SystemRoot%\servicing\
TrustedInstaller.exe,-101
Sun Apr 17 00:47:20 2016
Z,DeviceInstall\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,,
Sun Apr 17 00:44:02 2016 Z,BthLEEnum,@bthleenum.inf;%BthLEEnum.SVCDESC%;Bluetooth
Low Energy Driver,\SystemRoot\System32\drivers\BthLEEnum.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\BthHFSrv.dll,-102
Sun Apr 17 00:44:02 2016 Z,Parport,@msports.inf;%Parport.SVCDESC%;Parallel port
driver,\SystemRoot\System32\drivers\parport.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\p2psvc.dll,-8007
Sun Apr 17 00:44:02 2016 Z,Serenum,@msports.inf;%Serenum.SVCDESC%;Serenum Filter
Driver,\SystemRoot\System32\drivers\serenum.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Sun Apr 17 00:44:02 2016 Z,Serial,@msports.inf;%Serial.SVCDESC%;Serial port
driver,\SystemRoot\System32\drivers\serial.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Sun Apr 17 00:44:02 2016 Z,usbser,@usbser.inf;%UsbSerial.DriverDesc%;Microsoft USB
Serial Driver,\SystemRoot\System32\drivers\usbser.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Sun Apr 17 00:44:02 2016 Z,USBSTOR,@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass Storage
Driver,\SystemRoot\System32\drivers\USBSTOR.SYS,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Tue Apr 12 20:56:49 2016 Z,YahooAUService,Yahoo! Updater,"C:\Program Files
(x86)\Yahoo!\SoftwareUpdate\YahooAUService.exe",Own_Process,Auto
Start,LocalSystem,Keeps your favorite Yahoo! software up-to-date with the latest
features, tools, and enhancements.
Tue Apr  5 22:21:01 2016 Z,MSPCLOCK,@ksfilter.inf;%MSPCLOCK.DeviceDesc%;Microsoft
Streaming Clock Proxy,\SystemRoot\system32\drivers\MSPCLOCK.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Tue Apr  5 22:21:00 2016 Z,MSPQM,@ksfilter.inf;%MSPQM.DeviceDesc%;Microsoft
Streaming Quality Manager Proxy,\SystemRoot\system32\drivers\MSPQM.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Sat Apr  2 16:10:08 2016 Z,BthAvrcpTg,@bthaudhid.inf;%BthAvrcpTg_SvcDesc%;Bluetooth
Audio/Video Remote Control HID,\SystemRoot\System32\drivers\BthAvrcpTg.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Sat Apr  2 16:08:56 2016 Z,BthPan,@bthpan.inf;%BthPan.DisplayName%;Bluetooth Device
(Personal Area Network),\SystemRoot\System32\drivers\bthpan.sys,Kernel
driver,Manual,,@bthpan.inf,%BthPan.DisplayName%;Bluetooth Device (Personal Area
Network)
Sat Apr  2 16:08:55 2016 Z,BthEnum,@bth.inf;%BthEnum.SVCDESC%;Bluetooth Enumerator
Service,\SystemRoot\System32\drivers\BthEnum.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Sat Apr  2 16:08:55 2016 Z,RFCOMM,@tdibth.inf;%RFCOMM.DisplayName%;Bluetooth Device
(RFCOMM Protocol TDI),\SystemRoot\System32\drivers\rfcomm.sys,Kernel
driver,Manual,,@tdibth.inf,%RFCOMM.DisplayName%;Bluetooth Device (RFCOMM Protocol
TDI)
Tue Mar 29 09:31:18 2016
Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,System32\DRIVERS\ndistapi.sys,Ke
rnel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001
Tue Mar 29 09:31:18 2016
Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,\SystemRoot\System32\drivers\ndis
wan.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002
Tue Mar 29 09:31:18 2016
Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,\SystemRoot\System32\drivers
\raspptp.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32006
Tue Mar 29 09:31:18 2016
Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,\SystemRoot\System32\drivers\rasl
2tp.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32005
Tue Mar 29 09:31:18 2016
Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,\SystemRoot\System32\drivers\ras
pppoe.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32007
Tue Mar 29 09:31:17 2016 Z,RasAgileVpn,@netavpna.inf;%Svc-Mp-AgileVpn-DispName%;WAN
Page 98

SYSTEM OUTPUT.txt
Miniport (IKEv2),\SystemRoot\System32\drivers\AgileVpn.sys,Kernel
driver,Manual,,@netavpna.inf,%Svc-Mp-AgileVpn-DispName%;WAN Miniport (IKEv2)
Tue Mar 29 09:31:16 2016
Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,\SystemRoot\System32\drivers\rasss
tp.sys,Kernel driver,Manual,,@%systemroot%\system32\sstpsvc.dll,-202
Tue Mar 29 09:29:40 2016
Z,DeviceAssociationService,@%SystemRoot%\system32\das.dll;-100,%SystemRoot%\system32
\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\das.dll,-101
Tue Mar 29 09:22:07 2016
Z,lltdio,@%SystemRoot%\system32\lltdres.dll;-6,system32\drivers\lltdio.sys,Kernel
driver,Auto Start,,@%SystemRoot%\system32\lltdres.dll,-6
Tue Mar 29 09:22:07 2016
Z,ndiswanlegacy,@%systemroot%\system32\rascfg.dll;-32014,System32\DRIVERS\ndiswan.sy
s,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32014
Tue Mar 29 09:22:07 2016
Z,rspndr,@%SystemRoot%\system32\lltdres.dll;-5,system32\drivers\rspndr.sys,Kernel
driver,Auto Start,,@%SystemRoot%\system32\lltdres.dll,-5
Tue Mar 29 09:22:07 2016
Z,wanarp,@%systemroot%\system32\rascfg.dll;-32011,System32\DRIVERS\wanarp.sys,Kernel
driver,Auto Start,,@%systemroot%\system32\rascfg.dll,-32011
Tue Mar 29 09:22:07 2016
Z,wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,System32\DRIVERS\wanarp.sys,Kern
el driver,Manual,,@%systemroot%\system32\rascfg.dll,-32012
Sun Mar 27 13:05:49 2016 Z,ESProtectionDriver,Malwarebytes
Anti-Exploit,\??\C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae64.sys,Kernel
driver,System Start,,ePower Service
Sun Mar 27 13:05:49 2016 Z,MbaeSvc,Malwarebytes Anti-Exploit Service,"C:\Program
Files (x86)\Malwarebytes Anti-Exploit\mbae-svc.exe",Own_Process,Auto
Start,LocalSystem,Malwarebytes Anti-Exploit Service
Wed Mar 23 10:11:59 2016 Z,OpenVPNService,OpenVPN Service,"C:\Program Files
(x86)\HMA! Pro
VPN\bin\openvpnserv.exe",Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\APHos
tRes.dll,-10001
Wed Mar 23 10:11:16 2016 Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,,
Wed Mar 23 10:11:15 2016 Z,ndproxy,@%SystemRoot%\system32\drivers\todo.sys;-101;NDIS
Proxy,System32\DRIVERS\NDProxy.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\todo.sys,-101
Wed Mar 23 09:50:47 2016 Z,BrSerIb,@oem20.inf;%BrSerIb.SvcDesc%;Brother Serial
Interface Driver(WDM),\SystemRoot\system32\DRIVERS\BrSerIb.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Wed Mar 23 09:50:47 2016 Z,BrUsbSIb,@oem20.inf;%BrUsbSIb.SvcDesc%;Brother Serial USB
Driver(WDM),\SystemRoot\system32\DRIVERS\BrUsbSIb.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Wed Mar 23 09:50:47 2016 Z,usbprint,@usbprint.inf;%USBPRINT.SvcDesc%;Microsoft USB
PRINTER Class,\SystemRoot\System32\drivers\usbprint.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:50:47 2016 Z,usbscan,@sti.inf;%usbscan.SvcDesc%;USB Scanner
Driver,\SystemRoot\system32\DRIVERS\usbscan.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:50:26 2016 Z,stornvme,@stornvme.inf;%StorNVMe_ServiceDesc%;Microsoft
Standard NVM Express Driver,System32\drivers\stornvme.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\wiaservc.dll,-10
Wed Mar 23 09:48:50 2016 Z,BthHFEnum,@bthhfenum.inf;%BthHFEnum.SVCDESC%;Bluetooth
Hands-Free Audio and Call Control HID
Enumerator,\SystemRoot\System32\drivers\bthhfenum.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Wed Mar 23 09:48:50 2016
Z,BthHFSrv,@%SystemRoot%\System32\BthHFSrv.dll;-103,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\BthHFSrv.dll,-102
Wed Mar 23 09:48:50 2016
Z,BthHFSrv\Parameters,,%SystemRoot%\System32\BthHFSrv.dll,,,,
Page 99

SYSTEM OUTPUT.txt
Wed Mar 23 09:48:50 2016 Z,BTHPORT,@bth.inf;%BTHPORT.SvcDesc%;Bluetooth Port
Driver,\SystemRoot\System32\Drivers\BTHport.sys,Kernel
driver,Manual,,@bthpan.inf,%BthPan.DisplayName%;Bluetooth Device (Personal Area
Network)
Wed Mar 23 09:48:50 2016
Z,buttonconverter,@buttonconverter.inf;%btnconv.SvcDesc%;Service for Portable Device
Control devices,\SystemRoot\System32\drivers\buttonconverter.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102
Wed Mar 23 09:48:50 2016 Z,drmkaud,@wdmaudio.inf;%drmkaud.SvcDesc%;Microsoft Trusted
Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel
driver,Manual,,@%systemroot%\system32\dps.dll,-501
Wed Mar 23 09:48:50 2016 Z,msgpiowin32,@msgpiowin32.inf;%GPIO.SvcDesc%;Common Driver
for Buttons; DockMode and Laptop/Slate
Indicator,\SystemRoot\System32\drivers\msgpiowin32.sys,Kernel
driver,Manual,,@comres.dll,-2798
Wed Mar 23 09:48:50 2016 Z,sdbus,,\SystemRoot\System32\drivers\sdbus.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\certprop.dll,-14
Wed Mar 23 09:48:50 2016 Z,usbehci,@usbport.inf;%EHCIMP.SvcDesc%;Microsoft USB 2.0
Enhanced Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbehci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:48:50 2016 Z,usbhub,@usbport.inf;%ROOTHUB.SvcDesc%;Microsoft USB
Standard Hub Driver,\SystemRoot\System32\drivers\usbhub.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:48:50 2016 Z,usbohci,@usbport.inf;%OHCIMP.SvcDesc%;Microsoft USB Open
Host Controller Miniport Driver,\SystemRoot\System32\drivers\usbohci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:48:50 2016 Z,usbuhci,@usbport.inf;%UHCIMP.SvcDesc%;Microsoft USB
Universal Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbuhci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Mar 23 09:41:44 2016 Z,BrYNSvc,BrYNSvc,"C:\Program Files
(x86)\Browny02\BrYNSvc.exe",Own_Process,Manual,LocalSystem,@%systemroot%\system32\br
owser.dll,-101
Wed Mar 23 09:25:17 2016
Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.exe -k
imgsvc,Own_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\wiaservc.dll,-10
Tue Mar 22 13:52:39 2016
Z,MsBridge,@%SystemRoot%\system32\bridgeres.dll;-1,System32\drivers\bridge.sys,Kerne
l driver,Manual,,@%SystemRoot%\system32\bridgeres.dll,-1
Tue Mar 22 13:52:38 2016 Z,Ndisuio,NDIS Usermode I/O
Protocol,system32\drivers\ndisuio.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001
Tue Mar 22 13:52:38 2016 Z,xboxgip,@xboxgip.inf;%XBOXGIP_Desc%;Xbox Game Input
Protocol Driver,\SystemRoot\System32\drivers\xboxgip.sys,Kernel
driver,Manual,,@xboxgip.inf,%XBOXGIP_Desc%;Xbox Game Input Protocol Driver
Tue Mar 22 13:31:01 2016 Z,CCDMonitorService,CCDMonitorService,C:\Program Files
(x86)\Acer\AOP Framework\CCDMonitorService.exe,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\bthserv.dll,-102
Tue Mar 22 13:31:00 2016 Z,ose,Office Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",Own_Process,Manual,LocalSystem,Saves
installation files used for updates and repairs and is required for the downloading
of Setup updates and Watson error reports.
Tue Mar 22 13:18:45 2016
Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\ikeext.dll,-502
Tue Mar 22 13:16:27 2016 Z,MSDTC Bridge 3.0.0.0,,,,,,@comres.dll,-2798
Tue Mar 22 13:16:27 2016 Z,MSDTC Bridge 4.0.0.0,,,,,,@comres.dll,-2798
Tue Mar 22 13:16:27 2016 Z,ServiceModelEndpoint
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Tue Mar 22 13:16:27 2016 Z,ServiceModelOperation
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Page 100

SYSTEM OUTPUT.txt
Tue Mar 22 13:16:27 2016 Z,ServiceModelService
3.0.0.0,,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Tue Mar 22 13:16:27 2016 Z,SMSvcHost
3.0.0.0,,,,,,@%SystemRoot%\System32\SmsRouterSvc.dll,-10002
Tue Mar 22 13:16:27 2016 Z,SMSvcHost
4.0.0.0,,,,,,@%SystemRoot%\System32\SmsRouterSvc.dll,-10002
Tue Mar 22 13:16:27 2016 Z,Windows Workflow Foundation
3.0.0.0,,,,,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240
Tue Mar 22 13:16:27 2016 Z,Windows Workflow Foundation
4.0.0.0,,,,,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240
Tue Mar 22 13:15:54 2016
Z,intaud_WaveExtensible,@oem8.inf;%INTAUD_WEX.SvcDesc%;Intel WiDi Audio
Device,\SystemRoot\system32\drivers\intelaud.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Tue Mar 22 13:15:48 2016 Z,MSKSSRV,@ksfilter.inf;%MSKSSRV.DeviceDesc%;Microsoft
Streaming Service Proxy,\SystemRoot\system32\drivers\MSKSSRV.sys,Kernel
driver,Manual,,This service filters e-mail messages on your computer
Tue Mar 22 13:15:48 2016 Z,MSTEE,@ksfilter.inf;%MSTEE.DeviceDesc%;Microsoft
Streaming Tee/Sink-to-Sink Converter,\SystemRoot\system32\drivers\MSTEE.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Tue Mar 22 13:15:31 2016 Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
Service,%SystemRoot%\system32\igfxCUIService.exe,Own_Process,Auto
Start,LocalSystem,Service for Intel(R) HD Graphics Control Panel
Tue Mar 22 13:06:05 2016
Z,iphlpsvc\Parameters,,%SystemRoot%\System32\iphlpsvc.dll,,,,
Tue Mar 22 12:21:54 2016
Z,EventLog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\wevtsvc.dll,-201
Tue Mar 22 12:20:09 2016 Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,,
Tue Mar 22 11:54:41 2016 Z,MBAMScheduler,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamscheduler.exe",Own_Process,Auto Start,LocalSystem,Malwarebytes
Anti-Malware scheduler
Tue Mar 22 11:54:39 2016 Z,MBAMService,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamservice.exe",Own_Process,Auto Start,LocalSystem,Malwarebytes
Anti-Malware service
Tue Mar 22 11:54:39 2016
Z,MBAMWebAccessControl,,\??\C:\Windows\system32\drivers\mwac.sys,File system
driver,Manual,,Malwarebytes Anti-Malware service
Tue Mar 22 11:54:38 2016
Z,MBAMProtector,,\??\C:\Windows\system32\drivers\mbam.sys,File system
driver,Manual,,Malwarebytes Anti-Exploit Service
Tue Mar 22 11:21:46 2016 Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own_Process,Manual,LocalSystem,Inte
l(R) Content Protection HECI Service - enables communication with the Content
Protection FW
Tue Mar 22 10:37:21 2016 Z,odserv,Microsoft Office Diagnostics Service,"C:\Program
Files (x86)\Common Files\Microsoft
Shared\OFFICE12\ODSERV.EXE",Own_Process,Manual,LocalSystem,Run portions of Microsoft
Office Diagnostics.
Fri Sep 11 09:45:22 2015
Z,WpdUpFltr,@%systemroot%\System32\drivers\WpdUpFltr.sys;-100,System32\drivers\WpdUp
Fltr.sys,Kernel driver,Manual,,@%systemroot%\System32\drivers\WpdUpFltr.sys,-100
Fri Sep 11 09:45:22 2015 Z,WUDFWpdFs,,\SystemRoot\system32\DRIVERS\WUDFRd.sys,Kernel
driver,Manual,\Driver\WudfRd,@%SystemRoot%\system32\wudfsvc.dll,-1001
Thu Aug 13 23:24:15 2015
Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\Search
Indexer.exe /Embedding,Own_Process,Auto
Start,LocalSystem,@%systemroot%\system32\SearchIndexer.exe,-104
Thu Aug 13 23:03:20 2015
Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,Own_Process,Manual,NT
AUTHORITY\NetworkService,@comres.dll,-2798
Thu Aug 13 22:52:11 2015 Z,UcmUcsi,@ucmucsi.inf;%UcmUcsi.ServiceName%;USB Connector
Page 101

SYSTEM OUTPUT.txt

Manager UCSI Client,\SystemRoot\System32\drivers\UcmUcsi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Thu Aug 13 22:37:27 2015 Z,ePowerSvc,ePower Service,"C:\Program Files\Acer\Acer
Power Management\ePowerSvc.exe",Own_Process,Manual,LocalSystem,ePower Service
Thu Aug 13 22:35:41 2015 Z,QALSvc,Quick Access Local Service,"C:\Program
Files\Acer\Acer Quick Access\QALSvc.exe",Own_Process,Manual,NT
AUTHORITY\LocalService,Quick Access Local Service
Thu Aug 13 22:35:41 2015 Z,QASvc,Quick Access Service,"C:\Program Files\Acer\Acer
Quick Access\QASvc.exe",Own_Process,Manual,LocalSystem,Quick Access Service
Thu Aug 13 22:34:01 2015 Z,Dashlane Upgrade Service,,"C:\Program Files
(x86)\Dashlane\Upgrade\DashlaneUpgradeService.exe",Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\drivers\dam.sys,-101
Thu Aug 13 22:33:48 2015 Z,Amazon 1Button App Service,Amazon 1Button App
Service,"c:\Program Files
(x86)\Amazon\Amazon1ButtonApp\Amazon1ButtonService64.Exe",Own_Process,Auto
Start,LocalSystem,The Amazon 1Button App Service provides easy Internet Explorer
access and automatic updates
Thu Aug 13 22:25:21 2015 Z,AtherosSvc,AtherosSvc,"C:\Program Files (x86)\Qualcomm
Atheros\Bluetooth Suite\adminservice.exe",Own_Process,Auto Start,LocalSystem,Atheros
BT Stack Service Agent
Thu Aug 13 22:21:05 2015 Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,,
Thu Aug 13 22:19:13 2015 Z,ICCS,Intel(R) Integrated Clock Controller Service -
Intel(R) ICCS,"C:\Program Files (x86)\Intel\Intel(R) Integrated Clock Controller
Service\ICCProxy.exe",Own_Process,Manual,LocalSystem,Intel(R) Integrated Clock
Controller Service - Intel(R) ICCS
Thu Aug 13 22:19:11 2015
Z,ialm,,,,,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Aug 13 22:15:02 2015 Z,Intel(R) Capability Licensing Service TCP IP
Interface,Intel(R) Capability Licensing Service TCP IP Interface,"C:\Program
Files\Intel\TXE
Components\TCS\SocketHeciServer.exe",Own_Process,Manual,LocalSystem,Version:
1.35.117.1
Thu Aug 13 22:13:17 2015
Z,HdAudAddService,@hdaudio.inf;%UAAFunctionDriverForHdAudio.SvcDesc%;Microsoft 1.1
UAA Function Driver for High Definition Audio
Service,\SystemRoot\system32\DRIVERS\HdAudio.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Thu Aug 13 22:06:38 2015 Z,ClipSVC\Parameters,,%SystemRoot%\System32\ClipSVC.dll,,,,
Thu Aug 13 21:56:11 2015
Z,wlanSvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\wlansvc.dll,-258
Thu Aug 13 21:55:42 2015 Z,acpipagr,@acpipagr.inf;%SvcDesc%;ACPI Processor
Aggregator Driver,\SystemRoot\System32\drivers\acpipagr.sys,Kernel driver,Manual,,
Thu Aug 13 21:55:42 2015
Z,iaLPSSi_GPIO,@ialpssi_gpio.inf;%iaLPSSi_GPIO.SVCDESC%;Intel(R) Serial IO GPIO
Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_GPIO.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Aug 13 21:55:42 2015
Z,iaLPSSi_I2C,@ialpssi_i2c.inf;%iaLPSSi_I2C.SVCDESC%;Intel(R) Serial IO I2C
Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_I2C.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Aug 13 21:55:42 2015
Z,TPM,@tpm.inf;%TPM%;TPM,\SystemRoot\system32\drivers\tpm.sys,Kernel
driver,Manual,,@tpm.inf,%TPMDesc%;TPM Driver
Thu Aug 13 21:54:58 2015 Z,SecureLine,Avast SecureLine,C:\Program Files\AVAST
Software\SecureLine\VpnSvc.exe,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\seclogon.dll,-7000
Thu Aug 13 21:54:41 2015 Z,3ware,,System32\drivers\3ware.sys,Kernel driver,Boot
Start,,
Thu Aug 13 21:54:41 2015 Z,ADP80XX,,System32\drivers\ADP80XX.SYS,Kernel driver,Boot
Start,,
Thu Aug 13 21:54:41 2015 Z,agp440,@machine.inf;%agp440_svcdesc%;Intel AGP Bus

Page 102

SYSTEM OUTPUT.txt

Filter,System32\drivers\agp440.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\afd.sys,-1000
Thu Aug 13 21:54:41 2015 Z,amdsata,,System32\drivers\amdsata.sys,Kernel driver,Boot
Start,,The Amazon 1Button App Service provides easy Internet Explorer access and
automatic updates
Thu Aug 13 21:54:41 2015 Z,amdsbs,,System32\drivers\amdsbs.sys,Kernel driver,Boot
Start,,The Amazon 1Button App Service provides easy Internet Explorer access and
automatic updates
Thu Aug 13 21:54:41 2015 Z,amdxata,,System32\drivers\amdxata.sys,Kernel driver,Boot
Start,,The Amazon 1Button App Service provides easy Internet Explorer access and
automatic updates
Thu Aug 13 21:54:41 2015 Z,arcsas,@arcsas.inf;%arcsas_ServiceName%;Adaptec
SAS/SATA-II RAID Storport's Miniport Driver,System32\drivers\arcsas.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\appxdeploymentserver.dll,-2
Thu Aug 13 21:54:41 2015 Z,atapi,@mshdc.inf;%idechannel.DeviceDesc%;IDE
Channel,System32\drivers\atapi.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\rascfg.dll,-32000
Thu Aug 13 21:54:41 2015 Z,b06bdrv,@netbvbda.inf;%vbd_srv_desc%;Broadcom NetXtreme
II VBD,System32\drivers\bxvbda.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\AxInstSV.dll,-104
Thu Aug 13 21:54:41 2015 Z,ebdrv,@netevbda.inf;%vbd_srv_desc%;QLogic 10 Gigabit
Ethernet Adapter VBD,System32\drivers\evbda.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\eapsvc.dll,-2
Thu Aug 13 21:54:41 2015
Z,EhStorTcgDrv,@ehstortcgdrv.inf;%EhStorTcgDrv.Desc%;Microsoft driver for storage
devices supporting IEEE 1667 and TCG
protocols,System32\drivers\EhStorTcgDrv.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\EhStorClass.sys,-101
Thu Aug 13 21:54:41 2015 Z,gagp30kx,@machine.inf;%gagp30kx_svcdesc%;Microsoft
Generic AGPv3.0 Filter for K8 Processor
Platforms,System32\drivers\gagp30kx.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\fvevol.sys,-100
Thu Aug 13 21:54:41 2015 Z,HpSAMD,,System32\drivers\HpSAMD.sys,Kernel driver,Boot
Start,,McAfee Home Network
Thu Aug 13 21:54:41 2015 Z,iaStorAV,@iastorav.inf;%iaStorAV.DeviceDesc%;Intel(R)
SATA RAID Controller Windows,System32\drivers\iaStorAV.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Aug 13 21:54:41 2015 Z,iaStorV,@iastorv.inf;%*PNP0600.DeviceDesc%;Intel RAID
Controller Windows 7,System32\drivers\iaStorV.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Thu Aug 13 21:54:41 2015 Z,intelide,,System32\drivers\intelide.sys,Kernel
driver,Boot Start,,Version: 1.35.117.1
Thu Aug 13 21:54:41 2015 Z,isapnp,,System32\drivers\isapnp.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Thu Aug 13 21:54:41 2015 Z,LSI_SAS,,System32\drivers\lsi_sas.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\lmhsvc.dll,-102
Thu Aug 13 21:54:41 2015 Z,LSI_SAS2i,,System32\drivers\lsi_sas2i.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\lmhsvc.dll,-102
Thu Aug 13 21:54:41 2015 Z,LSI_SAS3i,,System32\drivers\lsi_sas3i.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\lmhsvc.dll,-102
Thu Aug 13 21:54:41 2015 Z,LSI_SSS,,System32\drivers\lsi_sss.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\lmhsvc.dll,-102
Thu Aug 13 21:54:41 2015 Z,megasas,,System32\drivers\megasas.sys,Kernel driver,Boot
Start,,McAfee Proxy Service
Thu Aug 13 21:54:41 2015 Z,megasr,,System32\drivers\megasr.sys,Kernel driver,Boot
Start,,McAfee Proxy Service
Thu Aug 13 21:54:41 2015 Z,mvumis,,System32\drivers\mvumis.sys,Kernel driver,Boot
Start,,@%systemroot%\system32\drivers\mup.sys,-102
Thu Aug 13 21:54:41 2015 Z,nvraid,,System32\drivers\nvraid.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Thu Aug 13 21:54:41 2015 Z,nvstor,,System32\drivers\nvstor.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Thu Aug 13 21:54:41 2015 Z,nv_agp,@machine.inf;%agpnvidia_svcdesc%;NVIDIA nForce AGP

Page 103

SYSTEM OUTPUT.txt
Bus Filter,System32\drivers\nv_agp.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Thu Aug 13 21:54:41 2015 Z,pciide,,System32\drivers\pciide.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Thu Aug 13 21:54:41 2015 Z,pcmcia,,System32\drivers\pcmcia.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Thu Aug 13 21:54:41 2015 Z,percsas2i,,System32\drivers\percsas2i.sys,Kernel
driver,Boot Start,,Intel Security PEF Service
Thu Aug 13 21:54:41 2015 Z,percsas3i,,System32\drivers\percsas3i.sys,Kernel
driver,Boot Start,,Intel Security PEF Service
Thu Aug 13 21:54:41 2015 Z,sbp2port,@sbp2.inf;%sbp2_ServiceDesc%;SBP-2
Transport/Protocol Bus Driver,System32\drivers\sbp2port.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\samsrv.dll,-2
Thu Aug 13 21:54:41 2015 Z,SiSRaid2,,System32\drivers\SiSRaid2.sys,Kernel
driver,Boot Start,,@%SystemRoot%\System32\shsvcs.dll,-12289
Thu Aug 13 21:54:41 2015 Z,SiSRaid4,,System32\drivers\sisraid4.sys,Kernel
driver,Boot Start,,@%SystemRoot%\System32\shsvcs.dll,-12289
Thu Aug 13 21:54:41 2015 Z,stexstor,,System32\drivers\stexstor.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\windows.staterepository.dll,-2
Thu Aug 13 21:54:41 2015 Z,storflt,@wstorflt.inf;%service_desc%;Microsoft Hyper-V
Storage Accelerator,System32\drivers\vmstorfl.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\wiaservc.dll,-10
Thu Aug 13 21:54:41 2015 Z,storufs,@storufs.inf;%UfsServiceDesc%;Microsoft Universal
Flash Storage (UFS) Driver,System32\drivers\storufs.sys,Kernel driver,Boot
Start,,@%SystemRoot%\System32\StorSvc.dll,-101
Thu Aug 13 21:54:41 2015 Z,storvsc,,System32\drivers\storvsc.sys,Kernel driver,Boot
Start,,@%SystemRoot%\System32\StorSvc.dll,-101
Thu Aug 13 21:54:41 2015 Z,uagp35,@machine.inf;%uagp35_svcdesc%;Microsoft AGPv3.5
Filter,System32\drivers\uagp35.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Thu Aug 13 21:54:41 2015 Z,uliagpkx,@machine.inf;%uliagpkx_svcdesc%;Uli AGP Bus
Filter,System32\drivers\uliagpkx.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\ui0detect.exe,-102
Thu Aug 13 21:54:41 2015 Z,vmbus,@wvmbus.inf;%vmbus.SVCDESC%;Virtual Machine
Bus,System32\drivers\vmbus.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\vhf.sys,-101
Thu Aug 13 21:54:41 2015 Z,vsmraid,,System32\drivers\vsmraid.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101
Thu Aug 13 21:54:41 2015 Z,VSTXRAID,@vstxraid.inf;%Driver.DeviceDesc%;VIA StorX
Storage RAID Controller Windows Driver,System32\drivers\vstxraid.sys,Kernel
driver,Boot Start,,@%systemroot%\system32\vssvc.exe,-101
Thu Jul 16 04:12:19 2015 Z,WINUSB,@winusb.inf;%WINUSB_SvcDesc%;WinUsb
Driver,\SystemRoot\System32\drivers\WinUSB.SYS,Kernel
driver,Manual,,@%Systemroot%\system32\wsmsvc.dll,-102
Thu Jul 16 04:12:16 2015 Z,terminpt,@termmou.inf;%TermInpt.SVCDESC%;Microsoft Remote
Desktop Input Driver,\SystemRoot\System32\drivers\terminpt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\tcpipcfg.dll,-50004
Thu Jul 16 04:12:01 2015 Z,kbdhid,@keyboard.inf;%KBDHID.SvcDesc%;Keyboard HID
Driver,\SystemRoot\System32\drivers\kbdhid.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Thu Jul 16 04:11:59 2015 Z,WUDFRd,@hidbthle.inf;%WudfRdDisplayName%;Windows Driver
Foundation - User-mode Driver Framework
Reflector,\SystemRoot\System32\drivers\WUDFRd.sys,Kernel
driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106
Thu Jul 16 04:01:46 2015
Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System32\sv
chost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\TabSvc.dll,-101
Thu Jul 16 03:47:02 2015 Z,UEIPSvc,User Experience Improvement Program,"C:\Program
Files\Acer\User Experience Improvement
Program\Framework\UBTService.exe",Own_Process,Manual,LocalSystem,Reads/Writes UDF
1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)
Page 104

SYSTEM OUTPUT.txt
Thu Jul 16 03:46:19 2015 Z,MozillaMaintenance,Mozilla Maintenance
Service,"C:\Program Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe",Own_Process,Manual,LocalSystem,The Mozilla
Maintenance Service ensures that you have the latest and most secure version of
Mozilla Firefox on your computer. Keeping Firefox up to date is very important for
your online security, and Mozilla strongly recommends that you keep this service
enabled.
Thu Jul 16 03:44:48 2015
Z,GamesAppIntegrationService,GamesAppIntegrationService,"C:\Program Files
(x86)\WildTangent Games\App\GamesAppIntegrationService.exe",Own_Process,Auto
Start,LocalSystem,WT Games App Integration Services
Thu Jul 16 03:44:47 2015 Z,GamesAppService,GamesAppService,"C:\Program Files
(x86)\WildTangent Games\App\GamesAppService.exe",Own_Process,Manual,LocalSystem,WT
Games App Services
Thu Jul 16 03:41:07 2015
Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot%\Mi
crosoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\PresentationHost.exe,-3310
Thu Jul 16 03:40:55 2015 Z,.NET CLR Data,,,,,,
Thu Jul 16 03:40:55 2015 Z,.NET CLR Networking,,,,,,,
Thu Jul 16 03:40:55 2015
Z,clr_optimization_v2.0.50727_32,,,,,,,@%SystemRoot%\system32\ClipSVC.dll,-104
Thu Jul 16 03:40:55 2015
Z,clr_optimization_v2.0.50727_64,,,,,,,@%SystemRoot%\system32\ClipSVC.dll,-104
Thu Jul 16 03:34:32 2015
Z,PrintNotify,@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll;-1,%SystemRoo
t%\system32\svchost.exe -k
print,Share_Process,Manual,LocalSystem,@C:\Windows\system32\spool\drivers\x64\3\Prin
tConfig.dll,-2
Thu Jul 16 03:34:32 2015
Z,PrintNotify\Parameters,,C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll,,,
,
Thu Jul 16 03:32:47 2015 Z,WlanSvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,,
Thu Jul 16 03:32:44 2015
Z,NativeWifiP,@%SystemRoot%\System32\drivers\nwifi.sys;-101,system32\DRIVERS\nwifi.s
ys,Kernel driver,Manual,,@%systemroot%\system32\drivers\mup.sys,-102
Thu Jul 16 03:31:44 2015 Z,GPIOClx0101,Microsoft GPIO Class Extension
Driver,System32\Drivers\msgpioclx.sys,Kernel driver,Manual,,WT Games App Services
Thu Jul 16 03:31:44 2015 Z,SpbCx,Simple Peripheral Bus Support
Library,system32\drivers\SpbCx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\snmptrap.exe,-4
Fri Jul 10 13:19:52 2015
Z,NgcCtnrSvc\Parameters,,%SystemRoot%\System32\NgcCtnrSvc.dll,,,,
Fri Jul 10 13:19:52 2015 Z,VaultSvc\Parameters,,C:\Windows\System32\vaultsvc.dll,,,,
Fri Jul 10 13:14:47 2015
Z,RDPDR,@%SystemRoot%\System32\DRIVERS\rdpdr.sys;-100,System32\drivers\rdpdr.sys,Ker
nel driver,Manual,,@%SystemRoot%\System32\DRIVERS\rdpdr.sys,-101
Fri Jul 10 13:14:47 2015 Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,Kernel
driver,Manual,,@%systemroot%\system32\drprov.dll,-101
Fri Jul 10 13:14:47 2015
Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svchost.e
xe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\sensrsvc.dll,-1001
Fri Jul 10 13:14:47 2015
Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%SystemRoot%\system32
\umrdp.dll,-1001
Fri Jul 10 13:14:46 2015 Z,RDPUDD,,,,,,,@%systemroot%\system32\drprov.dll,-101
Fri Jul 10 13:14:46 2015
Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,,
Fri Jul 10 13:14:46 2015
Page 105

SYSTEM OUTPUT.txt
Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,,
Fri Jul 10 12:22:48 2015
Z,Synth3dVsc,,\SystemRoot\System32\drivers\Synth3dVsc.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\swprv.dll,-102
Fri Jul 10 12:22:47 2015 Z,dmvsc,,\SystemRoot\System32\drivers\dmvsc.sys,Kernel
driver,Manual,,@%systemroot%\system32\Windows.Internal.Management.dll,-101
Fri Jul 10 12:22:47 2015
Z,gencounter,@wgencounter.inf;%GenCounter.SVCDESC%;Microsoft Hyper-V Generation
Counter,\SystemRoot\System32\drivers\vmgencounter.sys,Kernel driver,Manual,,WT Games
App Services
Fri Jul 10 12:22:44 2015 Z,UASPStor,@uaspstor.inf;%UASPortName%;USB Attached SCSI
(UAS) Driver,\SystemRoot\System32\drivers\uaspstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Fri Jul 10 12:22:43 2015 Z,sdstor,@sdstor.inf;%sdstor_ServiceDesc%;SD Storage Port
Driver,\SystemRoot\System32\drivers\sdstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\sdrsvc.dll,-102
Fri Jul 10 12:22:41 2015 Z,npsvctrig,@npsvctrig.inf;%NPSVCTRIG.SvcDisplayName%;Named
pipe service trigger provider,\SystemRoot\System32\drivers\npsvctrig.sys,Kernel
driver,System Start,,@%SystemRoot%\System32\nlasvc.dll,-2
Fri Jul 10 12:22:39 2015
Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,\SystemRoot\System32\drivers\asy
ncmac.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32000
Fri Jul 10 12:22:25 2015 Z,IPMIDRV,,\SystemRoot\System32\drivers\IPMIDrv.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\iphlpsvc.dll,-501
Fri Jul 10 12:22:25 2015 Z,iScsiPrt,@iscsi.inf;%iScsiPortName%;iScsiPort
Driver,\SystemRoot\System32\drivers\msiscsi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Fri Jul 10 12:22:22 2015 Z,HidBatt,@hidbatt.inf;%HidBatt.SvcDesc%;HID UPS Battery
Driver,\SystemRoot\System32\drivers\HidBatt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Fri Jul 10 12:22:22 2015
Z,mshidumdf,@%SystemRoot%\system32\drivers\mshidumdf.sys;-100,\SystemRoot\System32\d
rivers\mshidumdf.sys,Kernel driver,Manual,,@comres.dll,-2798
Fri Jul 10 12:22:21 2015 Z,fdc,@fdc.inf;%fdc_ServiceDesc%;Floppy Disk Controller
Driver,\SystemRoot\System32\drivers\fdc.sys,Kernel
driver,Manual,,@%systemroot%\system32\fxsresm.dll,-122
Fri Jul 10 12:22:21 2015 Z,flpydisk,@flpydisk.inf;%floppy_ServiceDesc%;Floppy Disk
Driver,\SystemRoot\System32\drivers\flpydisk.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000
Fri Jul 10 12:22:21 2015 Z,sfloppy,@flpydisk.inf;%sfloppy_devdesc%;High-Capacity
Floppy Disk Drive,\SystemRoot\System32\drivers\sfloppy.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Fri Jul 10 12:22:20 2015 Z,CapImg,@capimg.inf;%CapImgHid_Service%;HID driver for
CapImg touch screen,\SystemRoot\System32\drivers\capimg.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102
Fri Jul 10 12:22:19 2015 Z,BTHMODEM,@bthspp.inf;%BthSerial.DisplayName%;Bluetooth
Serial Communications Driver,\SystemRoot\System32\drivers\bthmodem.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\BthHFSrv.dll,-102
Fri Jul 10 12:22:18 2015 Z,bthhfhid,@bthaudhid.inf;%BthAudioHFHid.SVCDESC%;Bluetooth
Hands-Free Call Control HID,\SystemRoot\System32\drivers\BthHFHid.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Fri Jul 10 12:22:16 2015 Z,1394ohci,@1394.inf;%PCI\CC_0C0010.DeviceDesc%;1394 OHCI
Compliant Host Controller,\SystemRoot\System32\drivers\1394ohci.sys,Kernel
driver,Manual,,
Fri Jul 10 12:22:16 2015 Z,AcpiPmi,@acpipmi.inf;%AcpiPmi.SvcDesc%;ACPI Power Meter
Driver,\SystemRoot\System32\drivers\acpipmi.sys,Kernel driver,Manual,,
Fri Jul 10 12:22:08 2015
Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\wuaueng.dll,-106
Fri Jul 10 12:21:44 2015
Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchost.ex
e -k NetSvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\iphlpsvc.dll,-501
Page 106

SYSTEM OUTPUT.txt
Fri Jul 10 12:21:44 2015
Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\srvsvc.dll,-101
Fri Jul 10 12:21:43 2015 Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel
driver,Auto Start,,@%SystemRoot%\system32\drivers\pdc.sys,-101
Fri Jul 10 12:21:43 2015 Z,srvnet,,System32\DRIVERS\srvnet.sys,File system
driver,Manual,,@%systemroot%\system32\srvsvc.dll,-105
Fri Jul 10 12:21:42 2015
Z,MsLldp,@%SystemRoot%\system32\drivers\mslldp.sys;-200,system32\drivers\mslldp.sys,
Kernel driver,Auto Start,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Fri Jul 10 12:21:37 2015 Z,crypt32,,,,,,,Intel(R) Content Protection HECI Service -
enables communication with the Content Protection FW
Fri Jul 10 12:21:24 2015
Z,hyperkbd,,\SystemRoot\System32\drivers\hyperkbd.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Fri Jul 10 12:21:24 2015
Z,HyperVideo,,\SystemRoot\system32\DRIVERS\HyperVideo.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Fri Jul 10 12:21:24 2015 Z,netvsc,,\SystemRoot\System32\drivers\netvsc.sys,Kernel
driver,Manual,,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstal
lRC.dll,-8200
Fri Jul 10 12:21:24 2015 Z,s3cap,,\SystemRoot\System32\drivers\vms3cap.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lltdres.dll,-5
Fri Jul 10 12:21:24 2015
Z,VMBusHID,,\SystemRoot\System32\drivers\VMBusHID.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\vhf.sys,-101
Fri Jul 10 12:21:21 2015
Z,cnghwassist,@%SystemRoot%\system32\drivers\cnghwassist.sys;-100,System32\DRIVERS\c
nghwassist.sys,Kernel
driver,Disabled,,@%SystemRoot%\system32\drivers\cnghwassist.sys,-100
Fri Jul 10 12:20:51 2015
Z,NETVSCVFPP,,,,,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelIns
tallRC.dll,-8200
Fri Jul 10 12:20:44 2015
Z,NetSetupSvc,@%SystemRoot%\system32\NetSetupSvc.dll;-3,%SystemRoot%\System32\svchos
t.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\NetSetupSvc.dll,-4
Fri Jul 10 12:20:30 2015
Z,Psched,@%windir%\System32\drivers\pacer.sys;-101,System32\drivers\pacer.sys,Kernel
driver,System Start,,@%windir%\System32\drivers\pacer.sys,-101
Fri Jul 10 12:20:30 2015
Z,vwififlt,@%SystemRoot%\System32\drivers\vwififlt.sys;-259,System32\drivers\vwififl
t.sys,Kernel driver,System Start,,@%SystemRoot%\System32\drivers\vwififlt.sys,-260
Fri Jul 10 12:20:26 2015
Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50003
Fri Jul 10 12:20:26 2015 Z,Tcpip6,@todo.dll;-100;Microsoft IPv6 Protocol
Driver,System32\drivers\tcpip.sys,Kernel driver,Manual,,@todo.dll,-100;Microsoft
IPv6 Protocol Driver
Fri Jul 10 12:20:26 2015 Z,TCPIP6TUNNEL,,,,,,@todo.dll,-100;Microsoft IPv6 Protocol
Driver
Fri Jul 10 12:20:26 2015 Z,TCPIPTUNNEL,,,,,,Provides compatibility for legacy
applications which interact with TCP/IP through the registry. If this service is
stopped, certain applications may have impaired functionality.
Fri Jul 10 12:20:26 2015
Z,WFPLWFS,@%SystemRoot%\System32\drivers\wfplwfs.sys;-6000,System32\drivers\wfplwfs.
sys,Kernel driver,Boot Start,,@%SystemRoot%\System32\drivers\wfplwfs.sys,-6000
Fri Jul 10 12:20:23 2015 Z,acpiex,Microsoft ACPIEx
Driver,System32\Drivers\acpiex.sys,Kernel driver,Boot Start,,
Fri Jul 10 12:20:23 2015 Z,Ucx01000,USB Host Support
Library,system32\drivers\ucx01000.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Page 107

SYSTEM OUTPUT.txt

Fri Jul 10 12:20:23 2015 Z,WindowsTrustedRT,Windows Trusted Execution Environment
Class Extension,system32\drivers\WindowsTrustedRT.sys,Kernel driver,Boot
Start,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240
Fri Jul 10 12:20:23 2015
Z,WindowsTrustedRTProxy,@WindowsTrustedRTProxy.inf;%WindowsTrustedRTProxy.SVCDESC%;M
icrosoft Windows Trusted Runtime Secure
Service,System32\drivers\WindowsTrustedRTProxy.sys,Kernel driver,Boot
Start,,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240
Fri Jul 10 11:06:22 2015
Z,AudioEndpointBuilder,@%SystemRoot%\system32\AudioEndpointBuilder.dll;-204,%SystemR
oot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\AudioEndpointBuilder.dll,-205
Fri Jul 10 11:06:22 2015
Z,Audiosrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\audiosrv.dll,-201
Fri Jul 10 11:06:22 2015
Z,MMCSS,@%systemroot%\system32\drivers\mmcss.sys;-100,\SystemRoot\system32\drivers\m
mcss.sys,Kernel driver,Auto Start,,@%systemroot%\system32\drivers\mmcss.sys,-101
Fri Jul 10 11:06:01 2015 Z,Winsock,,,,,,@%systemroot%\system32\wsmsvc.dll,-102
Fri Jul 10 11:05:46 2015
Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32\svc
host.exe -k NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%systemroot%\system32\wkssvc.dll,-101
Fri Jul 10 11:05:46 2015
Z,NdisImPlatform,@%SystemRoot%\System32\drivers\ndisimplatform.sys;-501,System32\dri
vers\NdisImPlatform.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\ndisimplatform.sys,-501
Fri Jul 10 11:05:46 2015
Z,NetBIOS,@%windir%\system32\drivers\netbios.sys;-503,system32\drivers\netbios.sys,F
ile system driver,System Start,,@%windir%\system32\drivers\netbios.sys,-502
Fri Jul 10 11:05:46 2015
Z,NetbiosSmb,,,,,,@%windir%\system32\drivers\netbios.sys,-502
Fri Jul 10 11:05:46 2015 Z,RDMANDK,,,,,,@%systemroot%\system32\wkssvc.dll,-1001
Fri Jul 10 11:05:25 2015
Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\afd.
sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\afd.sys,-1000
Fri Jul 10 11:05:25 2015
Z,ahcache,@%systemroot%\system32\drivers\ahcache.sys;-102,system32\DRIVERS\ahcache.s
ys,Kernel driver,System Start,,@%systemroot%\system32\drivers\ahcache.sys,-101
Fri Jul 10 11:05:25 2015
Z,AJRouter,@%SystemRoot%\system32\AJRouter.dll;-2,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\AJRouter.dll,-1
Fri Jul 10 11:05:25 2015
Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own_Process,
Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\Alg.exe,-113
Fri Jul 10 11:05:25 2015
Z,AppID,@%systemroot%\system32\srpapi.dll;-100,\SystemRoot\system32\drivers\appid.sy
s,Kernel driver,Manual,,@%systemroot%\system32\srpapi.dll,-101
Fri Jul 10 11:05:25 2015
Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
Authority\LocalService,@%systemroot%\system32\appidsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\appinfo.dll,-101
Fri Jul 10 11:05:25 2015
Z,AppReadiness,@%SystemRoot%\System32\AppReadiness.dll;-1000,%SystemRoot%\System32\s
vchost.exe -k
AppReadiness,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\AppReadiness.dl
l,-1001
Fri Jul 10 11:05:25 2015

Page 108

SYSTEM OUTPUT.txt

```
Z,AppXSvc,@%SystemRoot%\system32\appxdeploymentserver.dll;-1,%systemroot%\system32\s
vchost.exe -k
wsappx,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\appxdeploymentserver.
dll,-2
Fri Jul 10 11:05:25 2015
Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchost.ex
e -k
AxInstSVGroup,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\AxInstSV.dll,-
104
Fri Jul 10 11:05:25 2015
Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\system32\bdesvc.dll,-101
Fri Jul 10 11:05:25 2015 Z,Beep,Beep,,Kernel driver,System
Start,,@%SystemRoot%\system32\bdesvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\bfe.dll,-1002
Fri Jul 10 11:05:25 2015
Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,File
system driver,Manual,,@%systemroot%\system32\browser.dll,-103
Fri Jul 10 11:05:25 2015
Z,BrokerInfrastructure,@%windir%\system32\bisrv.dll;-100,%SystemRoot%\system32\svcho
st.exe -k DcomLaunch,Share_Process,Auto
Start,LocalSystem,@%windir%\system32\bisrv.dll,-101
Fri Jul 10 11:05:25 2015
Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\browser.dll,-101
Fri Jul 10 11:05:25 2015
Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\bthserv.dll,-102
Fri Jul 10 11:05:25 2015 Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,File system driver,Disabled,,ISO9660/Joliet File
System Reader for CD/DVDs. (Core) (All pieces)
Fri Jul 10 11:05:25 2015
Z,CDPSvc,@%SystemRoot%\system32\cdpsvc.dll;-100,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\cdpsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svchost.
exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\certprop.dll,-12
Fri Jul 10 11:05:25 2015
Z,CLFS,@%SystemRoot%\system32\drivers\clfs.sys;-100,System32\drivers\CLFS.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\clfs.sys,-101
Fri Jul 10 11:05:25 2015
Z,ClipSVC,@%SystemRoot%\system32\ClipSVC.dll;-103,%SystemRoot%\System32\svchost.exe
-k wsappx,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\ClipSVC.dll,-104
Fri Jul 10 11:05:25 2015 Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\ClipSVC.dll,-104
Fri Jul 10 11:05:25 2015
Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own_Process,Manual,LocalSystem,@co
mres.dll,-948
Fri Jul 10 11:05:25 2015 Z,condrv,Console Driver,System32\drivers\condrv.sys,Kernel
driver,Manual,,@comres.dll,-948
Fri Jul 10 11:05:25 2015
Z,CoreMessagingRegistrar,@%SystemRoot%\system32\coremessaging.dll;-1,%SystemRoot%\sy
stem32\svchost.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\coremessaging.dll,-2
Fri Jul 10 11:05:25 2015
Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svchost.e
```

Page 109

SYSTEM OUTPUT.txt
xe -k NetworkService,Share_Process,Auto Start,NT
Authority\NetworkService,@%SystemRoot%\system32\cryptsvc.dll,-1002
Fri Jul 10 11:05:25 2015
Z,dam,@%SystemRoot%\system32\drivers\dam.sys;-100,system32\drivers\dam.sys,Kernel
driver,System Start,,@%SystemRoot%\system32\drivers\dam.sys,-101
Fri Jul 10 11:05:25 2015
Z,DcomLaunch,@combase.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem,@combase.dll,-5013
Fri Jul 10 11:05:25 2015
Z,DcpSvc,@%SystemRoot%\system32\dcpsvc.dll;-3001,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\dcpsvc.dll,-3002
Fri Jul 10 11:05:25 2015
Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svchost.
exe -k
defragsvc,Own_Process,Manual,localSystem,@%SystemRoot%\system32\defragsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,DeviceInstall,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svcho
st.exe -k
DcomLaunch,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\umpnpmgr.dll,-101
Fri Jul 10 11:05:25 2015
Z,DevQueryBroker,@%SystemRoot%\system32\DevQueryBroker.dll;-100,%SystemRoot%\system3
2\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\DevQueryBroker.dll,-101
Fri Jul 10 11:05:25 2015
Z,Dfsc,@%systemroot%\system32\wkssvc.dll;-1008,System32\Drivers\dfsc.sys,File system
driver,System Start,,@%systemroot%\system32\wkssvc.dll,-1009
Fri Jul 10 11:05:25 2015
Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\dhcpcore.dll,-101
Fri Jul 10 11:05:25 2015
Z,diagnosticshub.standardcollector.service,@%SystemRoot%\system32\DiagSvcs\Diagnosti
csHub.StandardCollector.ServiceRes.dll;-1000,%SystemRoot%\system32\DiagSvcs\Diagnost
icsHub.StandardCollector.Service.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\sy
stem32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1001
Fri Jul 10 11:05:25 2015
Z,DiagTrack,@%SystemRoot%\system32\diagtrack.dll;-3001,%SystemRoot%\System32\svchost
.exe -k utcsvc,Own_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\diagtrack.dll,-3002
Fri Jul 10 11:05:25 2015
Z,DmEnrollmentSvc,@%systemroot%\system32\Windows.Internal.Management.dll;-100,%syste
mroot%\system32\svchost.exe -k
netsvcs,Own_Process,Manual,LocalSystem,@%systemroot%\system32\Windows.Internal.Manag
ement.dll,-101
Fri Jul 10 11:05:25 2015
Z,dmwappushservice,@%SystemRoot%\system32\dmwappushsvc.dll;-200,%SystemRoot%\system3
2\svchost.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\dmwappushsvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.exe
-k NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\dnsapi.dll,-102
Fri Jul 10 11:05:25 2015
Z,DoSvc,@%systemroot%\system32\dosvc.dll;-100,%systemroot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%systemroot%\system32\dosvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%systemroot%\system32
\dot3svc.dll,-1103
Fri Jul 10 11:05:25 2015
Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
Page 110

SYSTEM OUTPUT.txt
LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\dps.dll,-501
Fri Jul 10 11:05:25 2015
Z,DsmSvc,@%SystemRoot%\system32\DeviceSetupManager.dll;-1000,%SystemRoot%\system32\s
vchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\DeviceSetupManager.d
ll,-1001
Fri Jul 10 11:05:25 2015
Z,DsSvc,@%SystemRoot%\system32\dssvc.dll;-10003,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\dssvc.dll,-10002
Fri Jul 10 11:05:25 2015 Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,,Controls
the underlying video driver stacks to provide fully-featured display capabilities.
Fri Jul 10 11:05:25 2015
Z,Eaphost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%systemroot%\system32\eapsvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Share_P
rocess,Manual,LocalSystem,@%SystemRoot%\system32\efssvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,embeddedmode,@%SystemRoot%\system32\embeddedmodesvc.dll;-200,%SystemRoot%\System32
\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\embeddedmodesvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,EntAppSvc,@EnterpriseAppMgmtSvc.dll;-1,%systemroot%\system32\svchost.exe -k
appmodel,Share_Process,Manual,LocalSystem,@EnterpriseAppMgmtSvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService,@comres.dll,-2451
Fri Jul 10 11:05:25 2015 Z,exfat,exFAT File System Driver,,File system
driver,Manual,,exFAT File System Driver
Fri Jul 10 11:05:25 2015 Z,fastfat,FAT12/16/32 File System Driver,,File system
driver,Manual,,Note - dependance on CDROM.SYS only if required to read/write DVD-RAM
media (which appears as CD class device). (Core) (All pieces)
Fri Jul 10 11:05:25 2015
Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,Own_P
rocess,Manual,NT AUTHORITY\NetworkService,@%systemroot%\system32\fxsresm.dll,-122
Fri Jul 10 11:05:25 2015
Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\fdPHost.dll,-101
Fri Jul 10 11:05:25 2015
Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\fdrespub.dll,-101
Fri Jul 10 11:05:25 2015
Z,fhsvc,@%systemroot%\system32\fhsvc.dll;-101,%SystemRoot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\fhsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,FileCrypt,@%systemroot%\system32\drivers\filecrypt.sys;-100,system32\drivers\filec
rypt.sys,File system driver,System
Start,,@%systemroot%\system32\drivers\filecrypt.sys,-101
Fri Jul 10 11:05:25 2015
Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,System32\drivers\fileinf
o.sys,File system driver,Boot
Start,,@%SystemRoot%\system32\drivers\fileinfo.sys,-101
Fri Jul 10 11:05:25 2015
Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers\fil
etrace.sys,File system
driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000
Page 111

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25 2015
Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmgr.sy
s,File system driver,Boot Start,,@%SystemRoot%\system32\drivers\fltmgr.sys,-10000
Fri Jul 10 11:05:25 2015
Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svchost.e
xe -k LocalService,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\FntCache.dll,-101
Fri Jul 10 11:05:25 2015
Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers\FsD
epends.sys,File system
driver,Manual,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000
Fri Jul 10 11:05:25 2015 Z,Fs_Rec,,,8,Boot
Start,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000
Fri Jul 10 11:05:25 2015 Z,gpsvc,@gpapi.dll;-112,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto Start,LocalSystem,@gpapi.dll,-113
Fri Jul 10 11:05:25 2015
Z,GpuEnergyDrv,@%SystemRoot%\system32\drivers\gpuenergydrv.sys;-100,System32\drivers
\gpuenergydrv.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Fri Jul 10 11:05:25 2015
Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\hidserv.dll,-102
Fri Jul 10 11:05:25 2015
Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System32\sv
chost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\ListSvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System32\sv
chost.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\provsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\http.sys,-2
Fri Jul 10 11:05:25 2015
Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwpolic
y.sys,Kernel driver,Boot Start,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Fri Jul 10 11:05:25 2015
Z,icssvc,@%SystemRoot%\System32\tetheringservice.dll;-4097,%SystemRoot%\system32\svc
host.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\System32\tetheringservice.dll,-4098
Fri Jul 10 11:05:25 2015
Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%SystemRo
ot%\system32\IEEtwCollector.exe
/V,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001
Fri Jul 10 11:05:25 2015
Z,IoQos,@%SystemRoot%\system32\drivers\ioqos.sys;-100,system32\drivers\ioqos.sys,Fil
e system driver,Manual,,@%SystemRoot%\system32\drivers\ioqos.sys,-101
Fri Jul 10 11:05:25 2015
Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipfltdrv.
sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32013
Fri Jul 10 11:05:25 2015 Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\iphlpsvc.dll,-501
Fri Jul 10 11:05:25 2015
Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.sys,
Kernel driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Fri Jul 10 11:05:25 2015
Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share_Process,Manual,Local
System,@keyiso.dll,-101
Fri Jul 10 11:05:25 2015 Z,KSecDD,,System32\Drivers\ksecdd.sys,Kernel driver,Boot
Page 112

SYSTEM OUTPUT.txt

Start,,@keyiso.dll,-101
Fri Jul 10 11:05:25 2015 Z,KSecPkg,,System32\Drivers\ksecpkg.sys,Kernel driver,Boot
Start,,@keyiso.dll,-101
Fri Jul 10 11:05:25 2015 Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\NetworkService,@comres.dll,-2947
Fri Jul 10 11:05:25 2015
Z,lfsvc,@%SystemRoot%\System32\lfsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\lfsvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,LicenseManager,@%SystemRoot%\system32\licensemanagersvc.dll;-200,%SystemRoot%\Syst
em32\svchost.exe -k LocalService,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\licensemanagersvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\lltdres.dll,-2
Fri Jul 10 11:05:25 2015
Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\lmhsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,LSM,@%windir%\system32\lsm.dll;-1001,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem,@%windir%\system32\lsm.dll,-1002
Fri Jul 10 11:05:25 2015
Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drivers\l
uafv.sys,File system driver,Auto
Start,,@%systemroot%\system32\drivers\luafv.sys,-101
Fri Jul 10 11:05:25 2015
Z,MapsBroker,@%SystemRoot%\System32\moshost.dll;-100,%SystemRoot%\System32\svchost.e
xe -k NetworkService,Own_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\moshost.dll,-101
Fri Jul 10 11:05:25 2015 Z,Modem,,system32\drivers\modem.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\mmcss.sys,-101
Fri Jul 10 11:05:25 2015
Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mountmg
r.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\mountmgr.sys,-101
Fri Jul 10 11:05:25 2015
Z,mpsdrv,@%SystemRoot%\system32\drivers\mpsdrv.sys;-23092,System32\drivers\mpsdrv.sy
s,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\mpsdrv.sys,-23093
Fri Jul 10 11:05:25 2015
Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svchost
.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\FirewallAPI.dll,-23091
Fri Jul 10 11:05:25 2015
Z,MRXDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mrxdav
.sys,File system driver,Manual,,@%systemroot%\system32\webclnt.dll,-105
Fri Jul 10 11:05:25 2015
Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,File
system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1003
Fri Jul 10 11:05:25 2015
Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys,Fil
e system driver,Auto Start,,@%systemroot%\system32\wkssvc.dll,-1005
Fri Jul 10 11:05:25 2015
Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys,Fil
e system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1007
Fri Jul 10 11:05:25 2015
Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchost.ex
e -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\iscsidsc.dll,-5001
Fri Jul 10 11:05:25 2015
Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.exe
/V,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\msimsg.dll,-32
Page 113

SYSTEM OUTPUT.txt
Fri Jul 10 11:05:25 2015
Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,File
system driver,Boot Start,,@%systemroot%\system32\drivers\mup.sys,-102
Fri Jul 10 11:05:25 2015
Z,NcaSvc,@%SystemRoot%\system32\ncasvc.dll;-3009,%SystemRoot%\System32\svchost.exe
-k NetSvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\ncasvc.dll,-3008
Fri Jul 10 11:05:25 2015
Z,NcbService,@%SystemRoot%\system32\ncbservice.dll;-500,%SystemRoot%\System32\svchos
t.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\ncbservice.dll,-501
Fri Jul 10 11:05:25 2015
Z,NcdAutoSetup,@%SystemRoot%\system32\NcdAutoSetup.dll;-100,%SystemRoot%\System32\sv
chost.exe -k LocalServiceNoNetwork,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\NcdAutoSetup.dll,-101
Fri Jul 10 11:05:25 2015
Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\ndis.sys,-201
Fri Jul 10 11:05:25 2015
Z,NdisCap,@%SystemRoot%\System32\drivers\ndiscap.sys;-5000,System32\drivers\ndiscap.
sys,Kernel driver,Manual,,@%SystemRoot%\System32\drivers\ndiscap.sys,-5000
Fri Jul 10 11:05:25 2015
Z,Ndu,@%SystemRoot%\system32\drivers\Ndu.sys;-10001,system32\drivers\Ndu.sys,Kernel
driver,Auto Start,,@%SystemRoot%\system32\drivers\Ndu.sys,-10002
Fri Jul 10 11:05:25 2015
Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,Kerne
l driver,System Start,,@%SystemRoot%\system32\drivers\netbt.sys,-1
Fri Jul 10 11:05:25 2015
Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.exe,
Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\netlogon.dll,-103
Fri Jul 10 11:05:25 2015
Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\netman.dll,-110
Fri Jul 10 11:05:25 2015
Z,netprofm,@%SystemRoot%\system32\netprofmsvc.dll;-202,%SystemRoot%\System32\svchost
.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\netprofmsvc.dll,-203
Fri Jul 10 11:05:25 2015
Z,NetTcpPortSharing,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelI
nstallRC.dll;-8201,%systemroot%\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,S
hare_Process,Disabled,NT
AUTHORITY\LocalService,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceMod
elInstallRC.dll,-8200
Fri Jul 10 11:05:25 2015
Z,NgcCtnrSvc,@%SystemRoot%\System32\NgcCtnrSvc.dll;-1,%SystemRoot%\system32\svchost.
exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\NgcCtnrSvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,NgcSvc,@%SystemRoot%\System32\ngcsvc.dll;-100,%SystemRoot%\system32\lsass.exe,Shar
e_Process,Manual,LocalSystem,@%SystemRoot%\System32\ngcsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\nlasvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\nsisvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsiproxy.
sys,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Jul 10 11:05:25 2015 Z,NTFS,,,File system
Page 114

SYSTEM OUTPUT.txt
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Jul 10 11:05:25 2015
Z,OneSyncSvc,@%SystemRoot%\system32\APHostRes.dll;-10002,%SystemRoot%\system32\svcho
st.exe -k UnistackSvcGroup,96,Auto
Start,LocalSystem,@%SystemRoot%\system32\APHostRes.dll,-10001
Fri Jul 10 11:05:25 2015
Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchost.ex
e -k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8005
Fri Jul 10 11:05:25 2015
Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\p2psvc.dll,-8007
Fri Jul 10 11:05:25 2015
Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\pcasvc.dll,-2
Fri Jul 10 11:05:25 2015 Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\pcasvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,pdc,@%SystemRoot%\system32\drivers\pdc.sys;-100,system32\drivers\pdc.sys,Kernel
driver,Boot Start,,@%SystemRoot%\system32\drivers\pdc.sys,-101
Fri Jul 10 11:05:25 2015
Z,PerfHost,@%systemroot%\sysWow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost.exe
,Own_Process,Manual,NT AUTHORITY\LocalService,@%systemroot%\SysWow64\perfhost.exe,-1
Fri Jul 10 11:05:25 2015
Z,PimIndexMaintenanceSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-15001,%System
Root%\system32\svchost.exe -k
UnistackSvcGroup,96,Manual,LocalSystem,@%SystemRoot%\system32\UserDataAccessRes.dll,
-15000
Fri Jul 10 11:05:25 2015
Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\pla.dll,-501
Fri Jul 10 11:05:25 2015
Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-200,%SystemRoot%\system32\svchost.ex
e -k
DcomLaunch,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\umpnpmgr.dll,-101
Fri Jul 10 11:05:25 2015
Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpauto.dll,-8003
Fri Jul 10 11:05:25 2015
Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8001
Fri Jul 10 11:05:25 2015
Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\svchos
t.exe -k NetworkServiceNetworkRestricted,Share_Process,Manual,NT
Authority\NetworkService,@%SystemRoot%\system32\polstore.dll,-5011
Fri Jul 10 11:05:25 2015
Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\umpo.dll,-101
Fri Jul 10 11:05:25 2015
Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\profsvc.dll,-301
Fri Jul 10 11:05:25 2015
Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\qwave.dll,-2
Fri Jul 10 11:05:25 2015
Page 115

SYSTEM OUTPUT.txt

Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\drive
rs\qwavedrv.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\qwavedrv.sys,-2
Fri Jul 10 11:05:25 2015
Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasauto.dll,-201
Fri Jul 10 11:05:25 2015
Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasmans.dll,-201
Fri Jul 10 11:05:25 2015
Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File
system driver,System Start,,@%systemroot%\system32\wkssvc.dll,-1001
Fri Jul 10 11:05:25 2015 Z,ReFSv1,,,File system driver,Manual,,ReadyBoost
Fri Jul 10 11:05:25 2015
Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svchost.
exe -k
netsvcs,Share_Process,Disabled,localSystem,@%Systemroot%\system32\mprdim.dll,-201
Fri Jul 10 11:05:25 2015
Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
localService,Share_Process,Disabled,NT AUTHORITY\LocalService,@regsvc.dll,-2
Fri Jul 10 11:05:25 2015
Z,RetailDemo,@%SystemRoot%\System32\RDXService.dll;-256,%SystemRoot%\System32\svchos
t.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\RDXService.dll,-257
Fri Jul 10 11:05:25 2015
Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svchost.e
xe -k RPCSS,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%windir%\system32\RpcEpMap.dll,-1002
Fri Jul 10 11:05:25 2015
Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator.exe
,Own_Process,Manual,NT
AUTHORITY\NetworkService,@%systemroot%\system32\Locator.exe,-3
Fri Jul 10 11:05:25 2015
Z,RpcSs,@combase.dll;-5010,%SystemRoot%\system32\svchost.exe -k
rpcss,Share_Process,Auto Start,NT AUTHORITY\NetworkService,@combase.dll,-5011
Fri Jul 10 11:05:25 2015
Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Share_P
rocess,Auto Start,LocalSystem,@%SystemRoot%\system32\samsrv.dll,-2
Fri Jul 10 11:05:25 2015
Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Disabled,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\SCardSvr.dll,-5
Fri Jul 10 11:05:25 2015
Z,ScDeviceEnum,@%SystemRoot%\System32\ScDeviceEnum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\ScDeviceEnum.dll,-101
Fri Jul 10 11:05:25 2015
Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfilter
.sys,Kernel driver,Manual,,@%SystemRoot%\System32\drivers\scfilter.sys,-12
Fri Jul 10 11:05:25 2015
Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchost.ex
e -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\schedsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svchost.
exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\certprop.dll,-14
Fri Jul 10 11:05:25 2015
Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.exe -k
SDRSVC,Own_Process,Manual,localSystem,@%SystemRoot%\system32\sdrsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.exe
-k

Page 116

SYSTEM OUTPUT.txt
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\seclogon.dll,-7000
Fri Jul 10 11:05:25 2015
Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\Sens.dll,-201
Fri Jul 10 11:05:25 2015
Z,SensorDataService,@%SystemRoot%\system32\SensorDataService.exe;-101,%SystemRoot%\S
ystem32\SensorDataService.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\
SensorDataService.exe,-102
Fri Jul 10 11:05:25 2015
Z,SensorService,@%SystemRoot%\System32\sensorservice.dll;-1000,%SystemRoot%\system32
\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\sensorservice.dll,-1001
Fri Jul 10 11:05:25 2015 Z,SerCx,Serial UART Support
Library,system32\drivers\SerCx.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Fri Jul 10 11:05:25 2015 Z,SerCx2,Serial UART Support
Library,system32\drivers\SerCx2.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Fri Jul 10 11:05:25 2015
Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svchost.
exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\SessEnv.dll,-1027
Fri Jul 10 11:05:25 2015
Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\svchos
t.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\ipnathlp.dll,-107
Fri Jul 10 11:05:25 2015
Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\shsvcs.dll,-12289
Fri Jul 10 11:05:25 2015
Z,smphost,@%SystemRoot%\System32\smphost.dll;-102,%SystemRoot%\System32\svchost.exe
-k smphost,Own_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\smphost.dll,-101
Fri Jul 10 11:05:25 2015
Z,SmsRouter,@%SystemRoot%\System32\SmsRouterSvc.dll;-10001,%SystemRoot%\system32\svc
host.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%SystemRoot%\System32
\SmsRouterSvc.dll,-10002
Fri Jul 10 11:05:25 2015
Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap.exe
,Own_Process,Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\snmptrap.exe,-4
Fri Jul 10 11:05:25 2015
Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.exe,Ow
n_Process,Auto Start,LocalSystem,@%systemroot%\system32\spoolsv.exe,-2
Fri Jul 10 11:05:25 2015
Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe,Own
_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\sppsvc.exe,-100
Fri Jul 10 11:05:25 2015
Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,File system
driver,Auto Start,,@%systemroot%\system32\srvsvc.dll,-103
Fri Jul 10 11:05:25 2015
Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,File system
driver,Manual,,@%systemroot%\system32\srvsvc.dll,-105
Fri Jul 10 11:05:25 2015
Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\ssdpsrv.dll,-101
Fri Jul 10 11:05:25 2015
Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
Page 117

SYSTEM OUTPUT.txt
Authority\LocalService,@%SystemRoot%\system32\sstpsvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,StateRepository,@%SystemRoot%\system32\windows.staterepository.dll;-1,%SystemRoot%
\system32\svchost.exe -k
appmodel,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\windows.statereposi
tory.dll,-2
Fri Jul 10 11:05:25 2015
Z,storqosflt,@%SystemRoot%\System32\drivers\storqosflt.sys;-101,system32\drivers\sto
rqosflt.sys,File system driver,Auto
Start,,@%SystemRoot%\System32\drivers\storqosflt.sys,-102
Fri Jul 10 11:05:25 2015
Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32
\StorSvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,svsvc,@%SystemRoot%\system32\svsvc.dll;-101,%SystemRoot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\svsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe -k
swprv,Own_Process,Manual,LocalSystem,@%SystemRoot%\System32\swprv.dll,-102
Fri Jul 10 11:05:25 2015
Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\sysmain.dll,-1001
Fri Jul 10 11:05:25 2015
Z,SystemEventsBroker,@%windir%\system32\SystemEventsBrokerServer.dll;-1001,%SystemRo
ot%\system32\svchost.exe -k DcomLaunch,Share_Process,Auto
Start,LocalSystem,@%windir%\system32\SystemEventsBrokerServer.dll,-1002
Fri Jul 10 11:05:25 2015
Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchost.ex
e -k NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\tapisrv.dll,-10101
Fri Jul 10 11:05:25 2015 Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,,Provides
compatibility for legacy applications which interact with TCP/IP through the
registry. If this service is stopped, certain applications may have impaired
functionality.
Fri Jul 10 11:05:25 2015
Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,\SystemRoot\system32\DRIVERS\tdx.sy
s,Kernel driver,System Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50004
Fri Jul 10 11:05:25 2015
Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svchost.
exe -k NetworkService,Share_Process,Manual,NT
Authority\NetworkService,@%SystemRoot%\System32\termsrv.dll,-267
Fri Jul 10 11:05:25 2015
Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svchost
.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\themeservice.dll,-8193
Fri Jul 10 11:05:25 2015
Z,tiledatamodelsvc,@%SystemRoot%\system32\tileobjserver.dll;-1,%systemroot%\system32
\svchost.exe -k appmodel,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\tileobjserver.dll,-2
Fri Jul 10 11:05:25 2015
Z,TimeBroker,@%windir%\system32\TimeBrokerServer.dll;-1001,%SystemRoot%\system32\svc
host.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%windir%\system32\TimeBrokerServer.dll,-1002
Fri Jul 10 11:05:25 2015
Z,Trkwks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\trkwks.dll,-2
Fri Jul 10 11:05:25 2015
Page 118

SYSTEM OUTPUT.txt

Z,TsUsbFlt,@%SystemRoot%\system32\drivers\tsusbflt.sys;-1000,System32\drivers\TsUsbF
lt.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Fri Jul 10 11:05:25 2015 Z,UcmCx0101,USB Connector Manager KMDF Class
Extension,System32\Drivers\UcmCx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Fri Jul 10 11:05:25 2015 Z,UdeCx,USB Device Emulation Support
Library,system32\drivers\udecx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Fri Jul 10 11:05:25 2015 Z,udfs,udfs,system32\DRIVERS\udfs.sys,File system
driver,Disabled,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on
C/DVD discs. (Core) (All pieces)
Fri Jul 10 11:05:25 2015 Z,Ufx01000,USB Function Class
Extension,system32\drivers\ufx01000.sys,Kernel driver,Manual,,Reads/Writes UDF
1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)
Fri Jul 10 11:05:25 2015
Z,UIODetect,@%SystemRoot%\system32\uiOdetect.exe;-101,%SystemRoot%\system32\UIODetec
t.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\uiOdetect.exe,-102
Fri Jul 10 11:05:25 2015
Z,UnistoreSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-10003,%SystemRoot%\Syste
m32\svchost.exe -k
UnistackSvcGroup,96,Manual,LocalSystem,@%SystemRoot%\system32\UserDataAccessRes.dll,
-10002
Fri Jul 10 11:05:25 2015
Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\upnphost.dll,-214
Fri Jul 10 11:05:25 2015 Z,UrsCx01000,USB Role-Switch Support
Library,system32\drivers\urscx01000.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Fri Jul 10 11:05:25 2015
Z,UserDataSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-14001,%SystemRoot%\syste
m32\svchost.exe -k
UnistackSvcGroup,96,Manual,LocalSystem,@%SystemRoot%\system32\UserDataAccessRes.dll,
-14000
Fri Jul 10 11:05:25 2015
Z,UserManager,@%systemroot%\system32\usermgr.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\usermgr.dll,-101
Fri Jul 10 11:05:25 2015
Z,UsoSvc,@%systemroot%\system32\usocore.dll;-102,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\usocore.dll,-101
Fri Jul 10 11:05:25 2015
Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass.exe
,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\vaultsvc.dll,-1004
Fri Jul 10 11:05:25 2015
Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Process,
Manual,LocalSystem,@%SystemRoot%\system32\vds.exe,-112
Fri Jul 10 11:05:25 2015
Z,vhf,@%SystemRoot%\system32\drivers\vhf.sys;-100,\SystemRoot\System32\drivers\vhf.s
ys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\vhf.sys,-101
Fri Jul 10 11:05:25 2015
Z,vmicguestinterface,@%systemroot%\system32\icsvc.dll;-801,%systemroot%\system32\svc
host.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\icsvc.dll,-802
Fri Jul 10 11:05:25 2015
Z,vmicheartbeat,@%systemroot%\system32\icsvc.dll;-101,%systemroot%\system32\svchost.
exe -k
ICService,Share_Process,Manual,LocalSystem,@%systemroot%\system32\icsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,vmickvpexchange,@%systemroot%\system32\icsvc.dll;-201,%systemroot%\system32\svchos
t.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
Page 119

SYSTEM OUTPUT.txt

\icsvc.dll,-202
Fri Jul 10 11:05:25 2015
Z,vmicrdv,@%systemroot%\system32\icsvc.dll;-601,%systemroot%\system32\svchost.exe -k
ICService,Share_Process,Manual,LocalSystem,@%systemroot%\system32\icsvc.dll,-602
Fri Jul 10 11:05:25 2015
Z,vmicshutdown,@%systemroot%\system32\icsvc.dll;-301,%systemroot%\system32\svchost.e
xe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\icsvc.dll,-302
Fri Jul 10 11:05:25 2015
Z,vmictimesync,@%systemroot%\system32\icsvc.dll;-401,%systemroot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\icsvc.dll,-402
Fri Jul 10 11:05:25 2015
Z,vmicvmsession,@%systemroot%\system32\icsvc.dll;-901,%systemroot%\system32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\icsvc.dll,-902
Fri Jul 10 11:05:25 2015
Z,vmicvss,@%systemroot%\system32\icsvc.dll;-501,%systemroot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\icsvc.dll,-502
Fri Jul 10 11:05:25 2015
Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmgrx.s
ys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101
Fri Jul 10 11:05:25 2015
Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_Proc
ess,Manual,LocalSystem,@%systemroot%\system32\vssvc.exe,-101
Fri Jul 10 11:05:25 2015
Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\w32time.dll,-201
Fri Jul 10 11:05:25 2015
Z,WalletService,@%SystemRoot%\System32\WalletService.dll;-1000,%SystemRoot%\System32
\svchost.exe -k
appmodel,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\WalletService.dll,-
1001
Fri Jul 10 11:05:25 2015
Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbengine.
exe",Own_Process,Manual,localSystem,@%systemroot%\system32\wbengine.exe,-105
Fri Jul 10 11:05:25 2015
Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k
WbioSvcGroup,Share_Process,Manual,LocalSystem,@%systemroot%\system32\wbiosrvc.dll,-1
01
Fri Jul 10 11:05:25 2015
Z,wcmsvc,@%SystemRoot%\System32\wcmsvc.dll;-4097,%SystemRoot%\System32\svchost.exe
-k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\System32\wcmsvc.dll,-4098
Fri Jul 10 11:05:25 2015
Z,wcncsvc,@%SystemRoot%\System32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\wcncsvc.dll,-4
Fri Jul 10 11:05:25 2015
Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%\sys
tem32\svchost.exe -k wcssvc,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\WcsPlugInService.dll,-201
Fri Jul 10 11:05:25 2015
Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svchost.e
xe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\wdi.dll,-503
Fri Jul 10 11:05:25 2015
Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchost.ex
Page 120

SYSTEM OUTPUT.txt

```
e -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\wdi.dll,-501
Fri Jul 10 11:05:25 2015 Z,wdiwifi,WDI Driver
Framework,system32\DRIVERS\wdiwifi.sys,Kernel
driver,Manual,,@%systemroot%\system32\wdi.dll,-501
Fri Jul 10 11:05:25 2015 Z,WdNisSvc,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-320,"%ProgramFiles%\Windows
Defender\NisSrv.exe",Own_Process,Manual,NT
AUTHORITY\LocalService,@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-242
Fri Jul 10 11:05:25 2015
Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\webclnt.dll,-101
Fri Jul 10 11:05:25 2015
Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\wecsvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,WEPHOSTSVC,@%systemroot%\system32\wephostsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k WepHostSvcGroup,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\wephostsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\System32\
svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\wercplsupport.dll,-1
00
Fri Jul 10 11:05:25 2015
Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
WerSvcGroup,Own_Process,Manual,localSystem,@%SystemRoot%\System32\wersvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,WiaRpc,@%SystemRoot%\system32\wiarpc.dll;-2,%SystemRoot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wiarpc.dll,-1
Fri Jul 10 11:05:25 2015 Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,File
system driver,Manual,,WIM Image mount service driver
Fri Jul 10 11:05:25 2015
Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\system32\
svchost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\winhttp.dll,-101
Fri Jul 10 11:05:25 2015
Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,localSystem,@%Systemroot%\system32\wbem\wmisvc.dll,-204
Fri Jul 10 11:05:25 2015
Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%Systemroot%\system32\wsmsvc.dll,-102
Fri Jul 10 11:05:25 2015
Z,wlidsvc,@%SystemRoot%\system32\wlidsvc.dll;-100,%SystemRoot%\system32\svchost.exe
-k netvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\wlidsvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\wbem\
wmiApSrv.exe,Own_Process,Manual,localSystem,@%Systemroot%\system32\wbem\wmiapsrv.exe
,-111
Fri Jul 10 11:05:25 2015 Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe",Own_Process,Manual,NT
AUTHORITY\NetworkService,@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102
Fri Jul 10 11:05:25 2015 Z,Wof,Windows Overlay File System Filter Driver,,File
system driver,Boot Start,,@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102
Fri Jul 10 11:05:25 2015
Z,workfolderssvc,@%systemroot%\system32\workfolderssvc.dll;-102,%SystemRoot%\System3
```

Page 121

SYSTEM OUTPUT.txt

```
2\svchost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\workfolderssvc.dll,-101
Fri Jul 10 11:05:25 2015 Z,wpcfltr,Family Safety Filter
Driver,system32\DRIVERS\wpcfltr.sys,Kernel
driver,Manual,,@%systemroot%\system32\workfolderssvc.dll,-101
Fri Jul 10 11:05:25 2015
Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\svchos
t.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wpdbusenum.dll,-101
Fri Jul 10 11:05:25 2015
Z,WpnService,@%SystemRoot%\system32\wpnservice.dll;-1,%systemroot%\system32\svchost.
exe -k
wswpnservice,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\wpnservice.dll,
-2
Fri Jul 10 11:05:25 2015
Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\driv
ers\ws2ifsl.sys,Kernel
driver,Disabled,,@%systemroot%\System32\drivers\ws2ifsl.sys,-1000
Fri Jul 10 11:05:25 2015
Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\wscsvc.dll,-201
Fri Jul 10 11:05:25 2015
Z,WSService,@%SystemRoot%\system32\WSService.dll;-103,%SystemRoot%\System32\svchost.
exe -k
wsappx,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\WSService.dll,-104
Fri Jul 10 11:05:25 2015
Z,WudfPf,@%SystemRoot%\System32\drivers\Wudfpf.sys;-1000,system32\drivers\WudfPf.sys
,Kernel driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106
Fri Jul 10 11:05:25 2015
Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wudfsvc.dll,-1001
Fri Jul 10 11:05:25 2015
Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.exe
-k LocalServiceNoNetwork,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\System32\wwansvc.dll,-258
Fri Jul 10 11:05:25 2015
Z,XblAuthManager,@%systemroot%\system32\XblAuthManager.dll;-100,%SystemRoot%\system3
2\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\XblAuthManager.dll,-
101
Fri Jul 10 11:05:25 2015
Z,XblGameSave,@%systemroot%\system32\XblGameSave.dll;-100,%SystemRoot%\system32\svch
ost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\XblGameSave.dll,-101
Fri Jul 10 11:05:25 2015
Z,XboxNetApiSvc,@%systemroot%\system32\XboxNetApiSvc.dll;-100,%SystemRoot%\system32\
svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%systemroot%\system32\XboxNetApiSvc.dll,-1
01
Fri Jul 10 11:05:06 2015 Z,.NET CLR Networking 4.0.0.0,,,,,,
Fri Jul 10 11:05:06 2015 Z,.NET Data Provider for Oracle,,,,,,
Fri Jul 10 11:05:06 2015 Z,.NET Data Provider for SqlServer,,,,,,
Fri Jul 10 11:05:06 2015 Z,.NET Memory Cache 4.0,,,,,,
Fri Jul 10 11:05:06 2015 Z,.NETFramework,,,,,,
Fri Jul 10 11:05:06 2015 Z,ADOVMPPackage,,,,,,
Fri Jul 10 11:05:06 2015 Z,adsi,,,,,,
Fri Jul 10 11:05:06 2015
Z,AJRouter\Parameters,,%SystemRoot%\System32\AJRouter.dll,,,,
Fri Jul 10 11:05:06 2015
```

Page 122

SYSTEM OUTPUT.txt
Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,,
Fri Jul 10 11:05:06 2015
Z,AppReadiness\Parameters,,%SystemRoot%\system32\AppReadiness.dll,,,,
Fri Jul 10 11:05:06 2015
Z,AppXSvc\Parameters,,%SystemRoot%\system32\appxdeploymentserver.dll,,,,
Fri Jul 10 11:05:06 2015
Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\AudioEndpointBuilder.dll,,,
,
Fri Jul 10 11:05:06 2015
Z,Audiosrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,,
Fri Jul 10 11:05:06 2015
Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,,
Fri Jul 10 11:05:06 2015 Z,BattC,,,,,,@%SystemRoot%\system32\AxInstSV.dll,-104
Fri Jul 10 11:05:06 2015 Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,,
Fri Jul 10 11:05:06 2015 Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,,
Fri Jul 10 11:05:06 2015
Z,BrokerInfrastructure\Parameters,,%SystemRoot%\System32\bisrv.dll,,,,
Fri Jul 10 11:05:06 2015 Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,,
Fri Jul 10 11:05:06 2015 Z,CDPSvc\Parameters,,%SystemRoot%\System32\CDPSvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,
Fri Jul 10 11:05:06 2015
Z,clr_optimization_v4.0.30319_32,,,,,,@%SystemRoot%\system32\ClipSVC.dll,-104
Fri Jul 10 11:05:06 2015
Z,clr_optimization_v4.0.30319_64,,,,,,@%SystemRoot%\system32\ClipSVC.dll,-104
Fri Jul 10 11:05:06 2015
Z,CoreMessagingRegistrar\Parameters,,%SystemRoot%\system32\coremessaging.dll,,,,
Fri Jul 10 11:05:06 2015 Z,CoreUI,,,,,,@%SystemRoot%\system32\coremessaging.dll,-2
Fri Jul 10 11:05:06 2015
Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DCLocator,,,,,,@%SystemRoot%\system32\drivers\dam.sys,-101
Fri Jul 10 11:05:06 2015
Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,
Fri Jul 10 11:05:06 2015 Z,DcpSvc\Parameters,,%SystemRoot%\system32\dcpsvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DeviceAssociationService\Parameters,,%SystemRoot%\system32\das.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DevQueryBroker\Parameters,,%SystemRoot%\system32\DevQueryBroker.dll,,,,
Fri Jul 10 11:05:06 2015 Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DmEnrollmentSvc\Parameters,,%systemroot%\system32\Windows.Internal.Management.dll,
,,,
Fri Jul 10 11:05:06 2015
Z,dmwappushservice\Parameters,,%SystemRoot%\system32\dmwappushsvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,,
Fri Jul 10 11:05:06 2015 Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,,
Fri Jul 10 11:05:06 2015
Z,DsmSvc\Parameters,,%SystemRoot%\System32\DeviceSetupManager.dll,,,,
Fri Jul 10 11:05:06 2015 Z,DsSvc\Parameters,,%SystemRoot%\System32\DsSvc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,Eaphost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,EFS\Parameters,,%SystemRoot%\system32\efssvc.dll,,,,
Fri Jul 10 11:05:06 2015
Z,embeddedmode\Parameters,,%SystemRoot%\System32\embeddedmodesvc.dll,,,,
Fri Jul 10 11:05:06 2015

Page 123

SYSTEM OUTPUT.txt

Z,EntAppSvc\Parameters,,%SystemRoot%\system32\EnterpriseAppMgmtSvc.dll,,,,
Fri Jul 10 11:05:06 2015 Z,ESENT,,,,,,ePower Service
Fri Jul 10 11:05:05 2015 Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,,
Fri Jul 10 11:05:05 2015 Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,,
Fri Jul 10 11:05:05 2015
Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,,
Fri Jul 10 11:05:05 2015 Z,fhsvc\Parameters,,%SystemRoot%\system32\fhsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,,
Fri Jul 10 11:05:05 2015 Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,,
Fri Jul 10 11:05:05 2015
Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,icssvc\Parameters,,%SystemRoot%\System32\tetheringservice.dll,,,,
Fri Jul 10 11:05:05 2015 Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,,
Fri Jul 10 11:05:05 2015 Z,inetaccs,,,,,,@%SystemRoot%\system32\ikeext.dll,-502
Fri Jul 10 11:05:05 2015 Z,KeyIso\Parameters,,%SystemRoot%\system32\keyiso.dll,,,,
Fri Jul 10 11:05:05 2015 Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,,
Fri Jul 10 11:05:05 2015
Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,ldap,,,,,,@%systemroot%\system32\wkssvc.dll,-101
Fri Jul 10 11:05:05 2015 Z,lfsvc\Parameters,,%SystemRoot%\System32\lfsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,LicenseManager\Parameters,,%SystemRoot%\system32\LicenseManagerSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Lsa,,,,,,@%SystemRoot%\system32\lmhsvc.dll,-102
Fri Jul 10 11:05:05 2015 Z,LSM\Parameters,,%SystemRoot%\System32\lsm.dll,,,,
Fri Jul 10 11:05:05 2015
Z,MapsBroker\Parameters,,%SystemRoot%\System32\moshost.dll,,,,
Fri Jul 10 11:05:05 2015 Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Msfs,,,File system driver,System Start,,@comres.dll,-2798
Fri Jul 10 11:05:05 2015
Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,,
Fri Jul 10 11:05:05 2015 Z,MsRPC,,,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Fri Jul 10 11:05:05 2015
Z,MSSCNTRS,,,,,,@%SystemRoot%\system32\drivers\mslldp.sys,-201
Fri Jul 10 11:05:05 2015 Z,napagent,,,,,,@%systemroot%\system32\drivers\mup.sys,-102
Fri Jul 10 11:05:05 2015 Z,NcaSvc\Parameters,,%SystemRoot%\System32\ncasvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,NcbService\Parameters,,%SystemRoot%\System32\ncbservice.dll,,,,
Fri Jul 10 11:05:05 2015
Z,NcdAutoSetup\Parameters,,%SystemRoot%\System32\NcdAutoSetup.dll,,,,
Fri Jul 10 11:05:05 2015
Z,Netlogon\Parameters,,%SystemRoot%\system32\netlogon.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,,
Fri Jul 10 11:05:05 2015
Z,netprofm\Parameters,,%SystemRoot%\System32\netprofmsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,NetSetupSvc\Parameters,,%SystemRoot%\System32\NetSetupSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,NgcSvc\Parameters,,%SystemRoot%\system32\ngcsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Npfs,,,File system driver,System
Start,,@%SystemRoot%\System32\nlasvc.dll,-2
Fri Jul 10 11:05:05 2015 Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,NTDS,,,,,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Jul 10 11:05:05 2015 Z,Null,,,Kernel driver,System
Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Jul 10 11:05:05 2015

Page 124

SYSTEM OUTPUT.txt
Z,OneSyncSvc\Parameters,,%SystemRoot%\System32\APHostService.dll,,,,
Fri Jul 10 11:05:05 2015
Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,PerfDisk,,,,,,Intel Security PEF Service
Fri Jul 10 11:05:05 2015 Z,PerfNet,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Fri Jul 10 11:05:05 2015 Z,PerfOS,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Fri Jul 10 11:05:05 2015 Z,PerfProc,,,,,,@%systemroot%\SysWow64\perfhost.exe,-1
Fri Jul 10 11:05:05 2015
Z,PimIndexMaintenanceSvc\Parameters,,%SystemRoot%\System32\PimIndexMaintenance.dll,,
,,
Fri Jul 10 11:05:05 2015 Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,,
Fri Jul 10 11:05:05 2015
Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,,
Fri Jul 10 11:05:05 2015
Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,,
Fri Jul 10 11:05:05 2015 Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,PortProxy,,,,,,@%SystemRoot%\system32\polstore.dll,-5011
Fri Jul 10 11:05:05 2015 Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,,
Fri Jul 10 11:05:05 2015 Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,,
Fri Jul 10 11:05:05 2015 Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,Kernel driver,Manual,,Remote Access Auto
Connection Driver
Fri Jul 10 11:05:05 2015 Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,,
Fri Jul 10 11:05:05 2015
Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,,,@%systemroot%\system32\drprov.dll
,-101
Fri Jul 10 11:05:05 2015
Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,,
Fri Jul 10 11:05:05 2015
Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,RetailDemo\Parameters,,%SystemRoot%\system32\RDXService.dll,,,,
Fri Jul 10 11:05:05 2015
Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,,
Fri Jul 10 11:05:05 2015 Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,,
Fri Jul 10 11:05:05 2015
Z,ScDeviceEnum\Parameters,,%SystemRoot%\System32\ScDeviceEnum.dll,,,,
Fri Jul 10 11:05:05 2015
Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,
Fri Jul 10 11:05:05 2015 Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,,
Fri Jul 10 11:05:05 2015 Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,,
Fri Jul 10 11:05:05 2015 Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SensorService\Parameters,,%SystemRoot%\system32\SensorService.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,,
Fri Jul 10 11:05:05 2015
Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,,
Fri Jul 10 11:05:05 2015 Z,smphost\Parameters,,%Systemroot%\System32\smphost.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SmsRouter\Parameters,,%SystemRoot%\system32\SmsRouterSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,,
Page 125

SYSTEM OUTPUT.txt
Fri Jul 10 11:05:05 2015 Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,StateRepository\Parameters,,%SystemRoot%\system32\windows.staterepository.dll,,,,
Fri Jul 10 11:05:05 2015 Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,svsvc\Parameters,,%SystemRoot%\system32\svsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,,
Fri Jul 10 11:05:05 2015 Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,,
Fri Jul 10 11:05:05 2015
Z,SystemEventsBroker\Parameters,,%SystemRoot%\System32\SystemEventsBrokerServer.dll,
,,,
Fri Jul 10 11:05:05 2015
Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,,
Fri Jul 10 11:05:05 2015
Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,,
Fri Jul 10 11:05:05 2015
Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,,
Fri Jul 10 11:05:05 2015
Z,tiledatamodelsvc\Parameters,,%SystemRoot%\system32\tileobjserver.dll,,,,
Fri Jul 10 11:05:05 2015
Z,TimeBroker\Parameters,,%SystemRoot%\System32\TimeBrokerServer.dll,,,,
Fri Jul 10 11:05:05 2015 Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,,
Fri Jul 10 11:05:05 2015
Z,TSDDD,,,,,,@%SystemRoot%\servicing\TrustedInstaller.exe,-101
Fri Jul 10 11:05:05 2015 Z,UGatherer,,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc
formats, usually found on C/DVD discs. (Core) (All pieces)
Fri Jul 10 11:05:05 2015 Z,UGTHRSVC,,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc
formats, usually found on C/DVD discs. (Core) (All pieces)
Fri Jul 10 11:05:05 2015
Z,UnistoreSvc\Parameters,,%SystemRoot%\System32\unistore.dll,,,,
Fri Jul 10 11:05:05 2015
Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,,
Fri Jul 10 11:05:05 2015
Z,UserDataSvc\Parameters,,%SystemRoot%\System32\userdataservice.dll,,,,
Fri Jul 10 11:05:05 2015
Z,UserManager\Parameters,,%SystemRoot%\System32\usermgr.dll,,,,
Fri Jul 10 11:05:05 2015 Z,UsoSvc\Parameters,,%systemroot%\system32\usocore.dll,,,,
Fri Jul 10 11:05:05 2015
Z,VerifierExt,@%SystemRoot%\system32\drivers\VerifierExt.sys;-1000,system32\drivers\
VerifierExt.sys,Kernel driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Fri Jul 10 11:05:05 2015
Z,vmicguestinterface\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,vmicheartbeat\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,vmickvpexchange\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,vmicrdv\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,vmicshutdown\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,vmictimesync\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,vmicvmsession\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,vmicvss\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WalletService\Parameters,,%SystemRoot%\system32\WalletService.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Wcmsvc\Parameters,,%SystemRoot%\System32\wcmsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,,
Page 126

SYSTEM OUTPUT.txt

```
Fri Jul 10 11:05:05 2015
Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,,
Fri Jul 10 11:05:05 2015 Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WEPHOSTSVC\Parameters,,%systemroot%\system32\wephostsvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WiaRpc\Parameters,,%SystemRoot%\System32\wiarpc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WinHttpAutoProxySvc\Parameters,,%SystemRoot%\system32\winhttp.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WinRM\Parameters,,%SystemRoot%\system32\wsmSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WinSock2,,,,,@%Systemroot%\system32\wsmsvc.dll,-102
Fri Jul 10 11:05:05 2015 Z,Wlidsvc\Parameters,,%SystemRoot%\system32\wlidsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WmiApRpl,,,,,@%SystemRoot%\system32\wlidsvc.dll,-101
Fri Jul 10 11:05:05 2015 Z,workerdd,,,,,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe,-102
Fri Jul 10 11:05:05 2015
Z,workfolderssvc\Parameters,,%systemroot%\system32\workfolderssvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,,
Fri Jul 10 11:05:05 2015
Z,Wpnservice\Parameters,,%SystemRoot%\system32\wpnservice.dll,,,,
Fri Jul 10 11:05:05 2015 Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WSearchIdxPi,,;,;,@%systemroot%\system32\SearchIndexer.exe,-104
Fri Jul 10 11:05:05 2015
Z,WSService\Parameters,,%SystemRoot%\System32\WSService.dll,,,,
Fri Jul 10 11:05:05 2015
Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,,
Fri Jul 10 11:05:05 2015 Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,,
Fri Jul 10 11:05:05 2015 Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,,
Fri Jul 10 11:05:05 2015
Z,Xbl AuthManager\Parameters,,%SystemRoot%\System32\XblAuthManager.dll,,,,
Fri Jul 10 11:05:05 2015
Z,XblGameSave\Parameters,,%SystemRoot%\System32\XblGameSave.dll,,,,
Fri Jul 10 11:05:05 2015
Z,XboxNetApiSvc\Parameters,,%SystemRoot%\system32\XboxNetApiSvc.dll,,,,
Fri Jul 10 11:04:15 2015
Z,xmlprov,,;,;,@%systemroot%\system32\XboxNetApiSvc.dll,-101
Fri Jul 10 11:04:15 2015
Z,TsUsbGD,@tsgenericusbdriver.inf;%TsUsbGD.DeviceDesc.Generic%;Remote Desktop
Generic USB Device,\SystemRoot\System32\drivers\TsUsbGD.sys,Kernel
driver,Manual,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Fri Jul 10 11:04:15 2015
Z,Urschipidea,@urschipidea.inf;%Urschipidea.ServiceName%;Chipidea USB Role-Switch
Driver,\SystemRoot\System32\drivers\urschipidea.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Fri Jul 10 11:04:15 2015
Z,UrsSynopsys,@urssynopsys.inf;%UrsSynopsys.ServiceName%;Synopsys USB Role-Switch
Driver,\SystemRoot\System32\drivers\urssynopsys.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Fri Jul 10 11:04:13 2015 Z,vhdmp,,\SystemRoot\System32\drivers\vhdmp.sys,Kernel
driver,Manual,@%SystemRoot%\system32\vds.exe,-112
Fri Jul 10 11:04:12 2015 Z,Amdk8,@cpu.inf;%Amdk8.SvcDesc%;AMD K8 Processor
Driver,\SystemRoot\System32\drivers\amdk8.sys,Kernel driver,Manual,,The Amazon
1Button App Service provides easy Internet Explorer access and automatic updates
Fri Jul 10 11:04:12 2015 Z,AmdPPM,@cpu.inf;%AmdPPM.SvcDesc%;AMD Processor
Driver,\SystemRoot\System32\drivers\amdppm.sys,Kernel driver,Manual,,The Amazon
```

Page 127

SYSTEM OUTPUT.txt

1Button App service provides easy Internet Explorer access and automatic updates
Fri Jul 10 11:04:12 2015 Z,Processor,@cpu.inf;%Processor.SvcDesc%;Processor
Driver,\SystemRoot\System32\drivers\processr.sys,Kernel
driver,Manual,,@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll,-2
Fri Jul 10 11:04:11 2015
z,UfxChipidea,@ufxchipidea.inf;%UfxChipidea.ServiceName%;USB Chipidea
Controller,\SystemRoot\System32\drivers\UfxChipidea.sys,Kernel
driver,Manual,,Reads/writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on
C/DVD discs.,(Core) (All pieces)
Fri Jul 10 11:04:11 2015
z,ufxsynopsys,@ufxsynopsys.inf;%ufxsynopsys.serviceName%;USB Synopsys
Controller,\SystemRoot\System32\drivers\ufxsynopsys.sys,Kernel
driver,Manual,,Reads/writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on
C/DVD discs.,(Core) (All pieces)
Fri Jul 10 11:04:08 2015 Z,ibbus,@m1x4_bus.inf;%Ibbus.ServiceDesc%;Mellanox
InfiniBand Bus/AL (Filter Driver),\SystemRoot\System32\drivers\ibbus.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Fri Jul 10 11:04:08 2015 Z,m1x4_bus,@m1x4_bus.inf;%MLX4BUS.ServiceDesc%;Mellanox
ConnectX Bus Enumerator,\SystemRoot\System32\drivers\m1x4_bus.sys,Kernel
driver,Manual,,Provides validation trust protection services
Fri Jul 10 11:04:08 2015 Z,ndfltr,@m1x4_bus.inf;%ndfltr.ServiceDesc%;NetworkDirect
service,\SystemRoot\System32\drivers\ndfltr.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\NcdAutoSetup.dll,-101
Fri Jul 10 11:04:08 2015 Z,sermouse,@msmouse.inf;%sermouse.SvcDesc%;Serial Mouse
Driver,\SystemRoot\System32\drivers\sermouse.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Fri Jul 10 11:04:08 2015 Z,WinMad,@m1x4_bus.inf;%WinMad.ServiceDesc%;WinMad
service,\SystemRoot\System32\drivers\winmad.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\winhttp.dll,-101
Fri Jul 10 11:04:08 2015 Z,WinVerbs,@m1x4_bus.inf;%WinVerbs.ServiceDesc%;WinVerbs
service,\SystemRoot\System32\drivers\winverbs.sys,Kernel
driver,Manual,,@%Systemroot%\system32\wsmsvc.dll,-102
Fri Jul 10 11:04:04 2015 Z,hidinterrupt,@hidinterrupt.inf;%HID.SvcDesc%;Common
Driver for HID Buttons implemented with
interrupts,\SystemRoot\System32\drivers\hidinterrupt.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Fri Jul 10 11:04:04 2015 Z,WacomPen,@hiddigi.inf;%WacomPen.SVCDESC%;Wacom Serial Pen
HID Driver,\SystemRoot\System32\drivers\wacompen.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\w32time.dll,-201
Fri Jul 10 11:04:03 2015 Z,acpitime,@acpitime.inf;%AcpiTime.SvcDesc%;ACPI Wake Alarm
Driver,\SystemRoot\System32\drivers\acpitime.sys,Kernel driver,Manual,,
Fri Jul 10 11:04:03 2015 Z,bcmfn2,@bcmfn2.inf;%bcmfn2.SVCDESC%;bcmfn2
service,\SystemRoot\System32\drivers\bcmfn2.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\AxInstSV.dll,-104
Fri Jul 10 11:04:03 2015 Z,ErrDev,@errdev.inf;%ERRDEV.SvcDesc%;Microsoft Hardware
Error Device Driver,\SystemRoot\System32\drivers\errdev.sys,Kernel
driver,Manual,,ePower Service
Fri Jul 10 11:04:03 2015
Z,genericusbfn,@genericusbfn.inf;%genericusbfn.serviceName%;Generic USB Function
Class,\SystemRoot\System32\drivers\genericusbfn.sys,Kernel driver,Manual,,WT Games
App Services
Fri Jul 10 11:04:01 2015 z,wfpcapture,@wfpcapture.inf;%WfpCapture_Desc%;Microsoft
WFP Message Capture,\SystemRoot\System32\drivers\wfpcapture.sys,Kernel
driver,Manual,,@wfpcapture.inf,%WfpCapture_Desc%;Microsoft WFP Message Capture
Fri Jul 10 11:04:01 2015 z,xinputhid,@xinputhid.inf;%xinputhid.SvcDesc%;XINPUT HID
Filter Driver,\SystemRoot\System32\drivers\xinputhid.sys,Kernel
driver,Manual,,@%systemroot%\system32\XboxNetApiSvc.dll,-101
Fri Jul 10 11:04:00 2015 Z,usbcir,@usbcir.inf;%usbcir.SVCDESC%;eHome Infrared
Receiver (USBCIR),\SystemRoot\System32\drivers\usbcir.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Fri Jul 10 11:03:59 2015 Z,circlass,@circlass.inf;%circlass.SVCDESC%;Consumer IR
Devices,\SystemRoot\System32\drivers\circlass.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\certprop.dll,-12
Page 128

SYSTEM OUTPUT.txt
Fri Jul 10 11:03:59 2015 Z,HidBth,@hidbth.inf;%HIDBTH.SvcDesc%;Microsoft Bluetooth
HID Miniport,\SystemRoot\System32\drivers\hidbth.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Fri Jul 10 11:03:59 2015 Z,HidIr,@hidir.inf;%HIDIR.SvcDesc%;Microsoft Infrared HID
Driver,\SystemRoot\System32\drivers\hidir.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-101
Fri Jul 10 11:03:58 2015 Z,fcvsc,,\SystemRoot\System32\drivers\fcvsc.sys,Kernel
driver,Manual,,@%systemroot%\system32\fxsresm.dll,-122
Fri Jul 10 11:03:58 2015 Z,vpci,@wvpci.inf;%vpci.SVCDESC%;Microsoft Hyper-V Virtual
PCI Bus,\SystemRoot\System32\drivers\vpci.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101
-------------------------------------------
Thu Apr 21 04:41:25 2016Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,Kernel driver,Manual,
Thu Apr 21 04:41:19 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common
Files\McAfee\SystemCore\\mfemms.exe",Own_Process,Auto Start,LocalSystem
Thu Apr 21 04:41:16 2016Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,
Thu Apr 21 04:41:15 2016Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor
Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",Own_Process,Auto
Start,LocalSystem
Thu Apr 21 04:41:15 2016Z,MCAPExe,McAfee AP Service,"C:\Program
Files\McAfee\MSC\MCAPExe.exe",Own_Process,Auto Start,LocalSystem
Thu Apr 21 04:41:15 2016Z,McMPFSvc,McAfee Personal Firewall Service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem
Thu Apr 21 04:41:15 2016Z,McProxy,McAfee Proxy Service,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto
Start,LocalSystem
Thu Apr 21 04:41:15
2016Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,
Thu Apr 21 03:24:59
2016Z,MBAMSwissArmy,MBAMSwissArmy,\??\C:\Windows\system32\drivers\MBAMSwissArmy.sys,
File system driver,Manual,
Thu Apr 21 03:20:08 2016Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,
Thu Apr 21 03:19:52 2016Z,cfwids,McAfee Inc.
cfwids,system32\drivers\cfwids.sys,Kernel driver,Manual,
Thu Apr 21 03:19:50 2016Z,mfencbdc,McAfee Inc.
mfencbdc,\SystemRoot\system32\DRIVERS\mfencbdc.sys,Kernel driver,Manual,
Thu Apr 21 03:19:31 2016Z,UmPass,@umpass.inf;%UmPass.SVCDESC%;Microsoft UMPass
Driver,\SystemRoot\System32\drivers\umpass.sys,Kernel driver,Manual,
Thu Apr 21 03:19:16 2016Z,tunnel,@nettun.inf;%TUNNEL.Service.DisplayName%;Microsoft
Tunnel Miniport Adapter Driver,\SystemRoot\System32\drivers\tunnel.sys,Kernel
driver,Manual,
Thu Apr 21 03:19:15
2016Z,vwifimp,@%SystemRoot%\System32\drivers\vwifimp.sys;-261,\SystemRoot\System32\d
rivers\vwifimp.sys,Kernel driver,Manual,
Thu Apr 21 03:19:03
2016Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,
Thu Apr 21 03:18:58
2016Z,BasicDisplay,,\SystemRoot\System32\drivers\BasicDisplay.sys,Kernel
driver,System Start,
Thu Apr 21 03:18:58 2016Z,monitor,@monitor.inf;%Monitor.SVCDESC%;Microsoft Monitor
Class Function Driver Service,\SystemRoot\System32\drivers\monitor.sys,Kernel
driver,Manual,
Thu Apr 21 03:18:57
2016Z,BtFilter,BtFilter,\SystemRoot\system32\DRIVERS\btfilter.sys,Kernel
driver,Manual,
Thu Apr 21 03:18:57 2016Z,BTHUSB,@bth.inf;%BTHUSB.SvcDesc%;Bluetooth Radio USB
Driver,\SystemRoot\System32\Drivers\BTHUSB.sys,Kernel driver,Manual,
Thu Apr 21 03:18:57 2016Z,RTSUER,@oem14.inf;%RtsUER%;Realtek USB Card Reader -
UER,\SystemRoot\system32\Drivers\RtsUer.sys,Kernel driver,Manual,
Page 129

SYSTEM OUTPUT.txt

Thu Apr 21 03:18:56 2016Z,Hidusb,@input.inf;%HID.SvcDesc%;Microsoft HID Class Driver,\SystemRoot\System32\drivers\hidusb.sys,Kernel driver,Manual,
Thu Apr 21 03:18:56 2016Z,usbccgp,@usb.inf;%GenericParent.SvcDesc%;Microsoft USB Generic Parent Driver,\SystemRoot\System32\drivers\usbccgp.sys,Kernel driver,Manual,
Thu Apr 21 03:18:56 2016Z,usbvideo,@usbvideo.inf;%USBVideo.SvcDesc%;USB Video Device (WDM),\SystemRoot\System32\Drivers\usbvideo.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,ETDI2C,@oem13.inf;%ELANI2CDeviceDesc%;ELAN I2C Filter Driver,\SystemRoot\System32\DRIVERS\ETDI2C.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,hidi2c,@hidi2c.inf;%hidi2c.SVCDESC%;Microsoft I2C HID Miniport Driver,\SystemRoot\System32\drivers\hidi2c.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,IntcDAud,@oem6.inf;%IntcDAud.SvcDesc%;Intel(R) Display Audio,\SystemRoot\system32\DRIVERS\IntcDAud.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,mouclass,@msmouse.inf;%mouclass.SvcDesc%;Mouse Class Driver,\SystemRoot\System32\drivers\mouclass.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,mouhid,@msmouse.inf;%MOUHID.SvcDesc%;Mouse HID Driver,\SystemRoot\System32\drivers\mouhid.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,mshidkmdf,,\SystemRoot\System32\drivers\mshidkmdf.sys,Kernel driver,Manual,
Thu Apr 21 03:18:55 2016Z,MTConfig,@mtconfig.inf;%MTConfig.SVCDESC%;Microsoft Input Configuration Driver,\SystemRoot\System32\drivers\MTConfig.sys,Kernel driver,Manual,
Thu Apr 21 03:18:54 2016Z,IntcAzAudAddService,Service for Realtek HD Audio (WDM),\SystemRoot\system32\drivers\RTKVHD64.sys,Kernel driver,Manual,
Thu Apr 21 03:18:54 2016Z,ksthunk,Kernel Streaming Thunks,\SystemRoot\system32\drivers\ksthunk.sys,Kernel driver,Manual,
Thu Apr 21 03:18:54 2016Z,USBHUB3,@usbhub3.inf;%UsbHub3.SVCDESC%;SuperSpeed Hub,\SystemRoot\System32\drivers\UsbHub3.sys,Kernel driver,Manual,
Thu Apr 21 03:18:51 2016Z,mssmbios,@mssmbios.inf;%mssmbios_svcdesc%;Microsoft System Management BIOS Driver,\SystemRoot\System32\drivers\mssmbios.sys,Kernel driver,System Start,
Thu Apr 21 03:18:49 2016Z,ACPI,@acpi.inf;%ACPI.SvcDesc%;Microsoft ACPI Driver,System32\drivers\ACPI.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,athr,@oem10.inf;%ATHR.Service.DispName%;Qualcomm Atheros Extensible Wireless LAN device driver,\SystemRoot\System32\drivers\athw10x.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,cdrom,@cdrom.inf;%cdrom_ServiceDesc%;CD-ROM Driver,\SystemRoot\System32\drivers\cdrom.sys,Kernel driver,System Start,
Thu Apr 21 03:18:49 2016Z,CmBatt,@cmbatt.inf;%CmBatt.SvcDesc%;Microsoft ACPI Control Method Battery Driver,\SystemRoot\System32\drivers\CmBatt.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,disk,@disk.inf;%disk_ServiceDesc%;Disk Driver,System32\drivers\disk.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,EhStorClass,@%SystemRoot%\system32\drivers\EhStorClass.sys;-100,System32\drive rs\EhStorClass.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol. sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,GPIO,@oem4.inf;%GPIO.SVCDESC%;Intel SoC GPIO Controller Driver,\SystemRoot\System32\drivers\iaiogpioe.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,HDAudBus,@hdaudbus.inf;%HDAudBus.SVCDESC%;Microsoft UAA Bus Driver for High Definition Audio,\SystemRoot\System32\drivers\HDAudBus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,i8042prt,@keyboard.inf;%i8042prt.SvcDesc%;i8042 Keyboard and PS/2 Mouse Port Driver,\SystemRoot\System32\drivers\i8042prt.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,iaioi2c,@oem5.inf;%Driver_Service_Desc%;I2C Controller Service,\SystemRoot\System32\drivers\iaioi2ce.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,igfx,,\SystemRoot\system32\DRIVERS\igdkmd64.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,intelpep,@intelpep.inf;%INTELPEP.SVCDESC%;Intel(R) Power Engine Plug-in Driver,System32\drivers\intelpep.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,intelppm,@cpu.inf;%IntelPPM.SvcDesc%;Intel Processor Driver,\SystemRoot\system32\drivers\intelppm.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,kbdclass,@keyboard.inf;%kbdclass.SvcDesc%;Keyboard Class

Page 130

SYSTEM OUTPUT.txt
Driver,\SystemRoot\System32\drivers\kbdclass.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,mfewfpk,McAfee Inc.
mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,msisadrv,,System32\drivers\msisadrv.sys,Kernel driver,Boot
Start,
Thu Apr 21 03:18:49
2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partm
gr.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,pci,@pci.inf;%pci_svcdesc%;PCI Bus
Driver,System32\drivers\pci.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel
driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,rt640x64,@oem12.inf;%rt640.Service.DispName%;Realtek RT640
NT Driver,\SystemRoot\System32\drivers\rt640x64.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49
2016Z,storahci,@mshdc.inf;%storahci_ServiceDescription%;Microsoft Standard SATA AHCI
Driver,System32\drivers\storahci.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,TXEIx64,@oem2.inf;%TEE_SvcDesc%;Intel(R) Trusted Execution
Engine Interface ,\SystemRoot\System32\drivers\TXEIx64.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,UEFI,@uefi.inf;%UEFI.SvcDesc%;Microsoft UEFI
Driver,\SystemRoot\System32\drivers\UEFI.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49 2016Z,USBXHCI,@usbxhci.inf;%PCI\CC_0C0330.DeviceDesc%;USB XHCI
Compliant Host Controller,\SystemRoot\System32\drivers\USBXHCI.SYS,Kernel
driver,Manual,
Thu Apr 21 03:18:49 2016Z,volsnap,@volume.inf;%VolumeClassName%;Storage
volumes,System32\drivers\volsnap.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49
2016Z,vwifibus,@%SystemRoot%\System32\drivers\vwifibus.sys;-257,\SystemRoot\System32
\drivers\vwifibus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:49
2016Z,Wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wd
f01000.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:49 2016Z,WmiAcpi,@wmiacpi.inf;%WMIMAP.SvcDesc%;Microsoft Windows
Management Interface for ACPI,\SystemRoot\System32\drivers\wmiacpi.sys,Kernel
driver,Manual,
Thu Apr 21 03:18:48
2016Z,BasicRender,,\SystemRoot\System32\drivers\BasicRender.sys,Kernel driver,System
Start,
Thu Apr 21 03:18:48
2016Z,CompositeBus,@compositebus.inf;%CompositeBus.SVCDESC%;Composite Bus Enumerator
Driver,\SystemRoot\System32\DriverStore\FileRepository\compositebus.inf_amd64_98334b
a6e76853ba\CompositeBus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,iwdbus,@oem9.inf;%iwdbus.SVCDESC%;IWD Bus
Enumerator,\SystemRoot\System32\drivers\iwdbus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,kdnic,@kdnic.inf;%KdNic.Service.DispName%;Microsoft Kernel
Debug Network Miniport (NDIS 6.20),\SystemRoot\System32\drivers\kdnic.sys,Kernel
driver,Manual,
Thu Apr 21 03:18:48 2016Z,LMDriver,@oem16.inf;%LMDriver.SVCDESC%;Launch Manager
Wireless Driver,\SystemRoot\System32\drivers\LMDriver.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48
2016Z,NdisVirtualBus,@%SystemRoot%\System32\drivers\NdisVirtualBus.sys;-200,\SystemR
oot\System32\drivers\NdisVirtualBus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,RadioShim,@oem16.inf;%RadioShim.SVCDESC%;Shim for HID-KMDF
Interface layer,\SystemRoot\System32\drivers\RadioShim.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,rdpbus,@rdpbus.inf;%rdpbus_svcdesc%;Remote Desktop Device
Redirector Bus Driver,\SystemRoot\System32\drivers\rdpbus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,spaceport,@spaceport.inf;%Spaceport_ServiceDesc%;Storage
Spaces Driver,System32\drivers\spaceport.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:48 2016Z,swenum,@swenum.inf;%SWENUM.SVCDESC%;Software Bus
Driver,\SystemRoot\System32\DriverStore\FileRepository\swenum.inf_amd64_2a699e44676b
7781\swenum.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016Z,tap0901,@oem23.inf;%DeviceDescription%;TAP-Windows Adapter
V9,\SystemRoot\System32\drivers\tap0901.sys,Kernel driver,Manual,
Page 131

```
SYSTEM OUTPUT.txt
Thu Apr 21 03:18:48 2016z,umbus,@umbus.inf;%umbus.SVCDESC%;UMBus Enumerator
Driver,\SystemRoot\System32\drivers\umbus.sys,Kernel driver,Manual,
Thu Apr 21 03:18:48 2016z,vdrvroot,@vdrvroot.inf;%vdrvroot_svcdesc%;Microsoft
Virtual Drive Enumerator,System32\drivers\vdrvroot.sys,Kernel driver,Boot Start,
Thu Apr 21 03:18:48 2016z,volmgr,@volmgr.inf;%volmgr_svcdesc%;Volume Manager
Driver,System32\drivers\volmgr.sys,Kernel driver,Boot Start,
Thu Apr 21 03:15:49 2016z,mfesapsn,McAfee Process Start Notification
service,\??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,Kernel
driver,Manual,
Thu Apr 21 03:15:18 2016z,McPvDrv,McPvDrv
Driver,\SystemRoot\system32\drivers\McPvDrv.sys,Kernel driver,Auto Start,
Thu Apr 21 03:15:06 2016z,MSK80Service,McAfee Anti-Spam service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem
Thu Apr 21 03:14:14 2016z,Hipshieldk,McAfee Inc.
Hipshieldk,system32\drivers\Hipshieldk.sys,Kernel driver,Manual,
Thu Apr 21 03:13:53 2016z,wdBoot,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-390,\SystemRoot\system32\drivers\WdBoot.sys,Kernel
driver,Manual,
Thu Apr 21 03:13:53 2016z,WdFilter,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-330,\SystemRoot\system32\drivers\WdFilter.sys,File system
driver,Manual,
Thu Apr 21 03:13:47 2016z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,Kernel driver,Boot Start,
Thu Apr 21 03:13:47 2016z,WinDefend,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-310,"%ProgramFiles%\Windows
Defender\MsMpEng.exe",Own_Process,Manual,LocalSystem
Thu Apr 21 03:13:46 2016z,WdNisDrv,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-370,system32\Drivers\WdNisDrv.sys,Kernel driver,Manual,
Thu Apr 21 03:13:35 2016z,MCODS,McAfee Scanner,"C:\Program
Files\McAfee\VirusScan\mcods.exe",Own_Process,Manual,LocalSystem
Thu Apr 21 03:13:25 2016z,McNaiAnn,McAfee VirusScan Announcer,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem
Thu Apr 21 03:12:49 2016z,mfencrk,McAfee Inc.
mfencrk,\SystemRoot\system32\DRIVERS\mfencrk.sys,Kernel driver,Manual,
Thu Apr 21 03:12:03 2016z,McBootDelayStartSvc,McAfee Boot Delay Start
service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSVHost.exe"
/McCoreSvc,Share_Process,Auto Start,LocalSystem
Thu Apr 21 03:12:02 2016z,mcpltsvc,McAfee Platform Services,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto
start,LocalSystem
Thu Apr 21 03:11:46 2016z,PEFService,Intel Security PEF Service,"C:\Program
Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",Own_Process,Auto
start,LocalSystem
Thu Apr 21 03:11:37 2016z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common
Files\McAfee\CSP\1.9.656.0\McCSPServiceHost.exe",Own_Process,Auto Start,LocalSystem
Thu Apr 21 03:10:59 2016z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto
start,LocalSystem
Thu Apr 21 03:10:58 2016z,mfefire,McAfee Firewall Core Service,"C:\Program
Files\Common Files\McAfee\SystemCore\mfefire.exe",Own_Process,Manual,LocalSystem
Thu Apr 21 03:10:57 2016z,mfevtp,McAfee Validation Trust Protection
service,"C:\Windows\system32\mfevtps.exe",Own_Process,Manual,LocalSystem
Thu Apr 21 03:10:48 2016z,mfeelamk,McAfee Inc.
mfeelamk,system32\drivers\mfeelamk.sys,Kernel driver,Boot Start,
Thu Apr 21 03:08:54 2016z,ModuleCoreService,McAfee Module Core Service,"C:\Program
Files\Common Files\McAfee\ModuleCore\ModuleCoreService.exe",Share_Process,Auto
start,LocalSystem
Thu Apr 21 03:00:51
2016z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Auto Start,LocalSystem
Sun Apr 17 00:48:02
```

Page 132

SYSTEM OUTPUT.txt
2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\TrustedInstaller.exe,Own_Process,Manual,localSystem
Sun Apr 17 00:47:20
2016Z,DeviceInstall\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Sun Apr 17 00:44:02 2016Z,BthLEEnum,@bthleenum.inf;%BthLEEnum.SVCDESC%;Bluetooth Low Energy Driver,\SystemRoot\System32\drivers\BthLEEnum.sys,Kernel driver,Manual, .
Sun Apr 17 00:44:02 2016Z,Parport,@msports.inf;%Parport.SVCDESC%;Parallel port driver,\SystemRoot\System32\drivers\parport.sys,Kernel driver,Manual,
Sun Apr 17 00:44:02 2016Z,Serenum,@msports.inf;%Serenum.SVCDESC%;Serenum Filter Driver,\SystemRoot\System32\drivers\serenum.sys,Kernel driver,Manual,
Sun Apr 17 00:44:02 2016Z,Serial,@msports.inf;%Serial.SVCDESC%;Serial port driver,\SystemRoot\System32\drivers\serial.sys,Kernel driver,Manual,
Sun Apr 17 00:44:02 2016Z,usbser,@usbser.inf;%UsbSerial.DriverDesc%;Microsoft USB Serial Driver,\SystemRoot\System32\drivers\usbser.sys,Kernel driver,Manual,
Sun Apr 17 00:44:02 2016Z,USBSTOR,@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass Storage Driver,\SystemRoot\System32\drivers\USBSTOR.SYS,Kernel driver,Manual,
Tue Apr 12 20:56:49 2016Z,YahooAUService,Yahoo! Updater,"C:\Program Files (x86)\Yahoo!\SoftwareUpdate\YahooAUService.exe",Own_Process,Auto Start,LocalSystem
Tue Apr 5 22:21:01 2016Z,MSPCLOCK,@ksfilter.inf;%MSPCLOCK.DeviceDesc%;Microsoft Streaming Clock Proxy,\SystemRoot\system32\drivers\MSPCLOCK.sys,Kernel driver,Manual,
Tue Apr 5 22:21:00 2016Z,MSPQM,@ksfilter.inf;%MSPQM.DeviceDesc%;Microsoft Streaming Quality Manager Proxy,\SystemRoot\system32\drivers\MSPQM.sys,Kernel driver,Manual,
Sat Apr 2 16:10:08 2016Z,BthAvrcpTg,@bthaudhid.inf;%BthAvrcpTg_SvcDesc%;Bluetooth Audio/Video Remote Control HID,\SystemRoot\System32\drivers\BthAvrcpTg.sys,Kernel driver,Manual,
Sat Apr 2 16:08:56 2016Z,BthPan,@bthpan.inf;%BthPan.DisplayName%;Bluetooth Device (Personal Area Network),\SystemRoot\System32\drivers\bthpan.sys,Kernel driver,Manual,
Sat Apr 2 16:08:55 2016Z,BthEnum,@bth.inf;%BthEnum.SVCDESC%;Bluetooth Enumerator Service,\SystemRoot\System32\drivers\BthEnum.sys,Kernel driver,Manual,
Sat Apr 2 16:08:55 2016Z,RFCOMM,@tdibth.inf;%RFCOMM.DisplayName%;Bluetooth Device (RFCOMM Protocol TDI),\SystemRoot\System32\drivers\rfcomm.sys,Kernel driver,Manual,
Tue Mar 29 09:31:18 2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,System32\DRIVERS\ndistapi.sys,Kernel driver,Manual,
Tue Mar 29 09:31:18 2016Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,\SystemRoot\System32\drivers\ndiswan.sys,Kernel driver,Manual,
Tue Mar 29 09:31:18 2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,\SystemRoot\System32\drivers\raspptp.sys,Kernel driver,Manual,
Tue Mar 29 09:31:18 2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,\SystemRoot\System32\drivers\rasl2tp.sys,Kernel driver,Manual,
Tue Mar 29 09:31:18 2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,\SystemRoot\System32\drivers\raspppoe.sys,Kernel driver,Manual,
Tue Mar 29 09:31:17 2016Z,RasAgileVpn,@netavpna.inf;%Svc-Mp-AgileVpn-DispName%;WAN Miniport (IKEv2),\SystemRoot\System32\drivers\AgileVpn.sys,Kernel driver,Manual,
Tue Mar 29 09:31:16 2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,\SystemRoot\System32\drivers\rassstp.sys,Kernel driver,Manual,
Tue Mar 29 09:29:40 2016Z,DeviceAssociationService,@%SystemRoot%\system32\das.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Mar 29 09:22:07 2016Z,lltdio,@%SystemRoot%\system32\lltdres.dll;-6,system32\drivers\lltdio.sys,Kernel driver,Auto Start,
Tue Mar 29 09:22:07 2016Z,ndiswanlegacy,@%systemroot%\system32\rascfg.dll;-32014,System32\DRIVERS\ndiswan.sys,Kernel driver,Manual,

Page 133

SYSTEM OUTPUT.txt

Tue Mar 29 09:22:07
2016Z,rspndr,@%SystemRoot%\system32\lltdres.dll;-5,system32\drivers\rspndr.sys,Kerne
l driver,Auto Start,
Tue Mar 29 09:22:07
2016Z,wanarp,@%systemroot%\system32\rascfg.dll;-32011,System32\DRIVERS\wanarp.sys,Ke
rnel driver,Auto Start,
Tue Mar 29 09:22:07
2016Z,wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,System32\DRIVERS\wanarp.sys,
Kernel driver,Manual,
Sun Mar 27 13:05:49 2016Z,ESProtectionDriver,Malwarebytes
Anti-Exploit,\??\C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae64.sys,Kernel
driver,System Start,
Sun Mar 27 13:05:49 2016Z,MbaeSvc,Malwarebytes Anti-Exploit Service,"C:\Program
Files (x86)\Malwarebytes Anti-Exploit\mbae-svc.exe",Own_Process,Auto
Start,LocalSystem
Wed Mar 23 10:11:59 2016Z,OpenVPNService,OpenVPN Service,"C:\Program Files
(x86)\HMA! Pro VPN\bin\openvpnserv.exe",Own_Process,Manual,LocalSystem
Wed Mar 23 10:11:16 2016Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Wed Mar 23 10:11:15 2016Z,ndproxy,@%SystemRoot%\system32\drivers\todo.sys;-101;NDIS
Proxy,System32\DRIVERS\NDProxy.sys,Kernel driver,Manual,
Wed Mar 23 09:50:47 2016Z,BrSerIb,@oem20.inf;%BrSerIb.SvcDesc%;Brother Serial
Interface Driver(WDM),\SystemRoot\system32\DRIVERS\BrSerIb.sys,Kernel driver,Manual,
Wed Mar 23 09:50:47 2016Z,BrUsbSIb,@oem20.inf;%BrUsbSIb.SvcDesc%;Brother Serial USB
Driver(WDM),\SystemRoot\system32\DRIVERS\BrUsbSIb.sys,Kernel driver,Manual,
Wed Mar 23 09:50:47 2016Z,usbprint,@usbprint.inf;%USBPRINT.SvcDesc%;Microsoft USB
PRINTER Class,\SystemRoot\System32\drivers\usbprint.sys,Kernel driver,Manual,
Wed Mar 23 09:50:47 2016Z,usbscan,@sti.inf;%usbscan.SvcDesc%;USB Scanner
Driver,\SystemRoot\system32\DRIVERS\usbscan.sys,Kernel driver,Manual,
Wed Mar 23 09:50:26 2016Z,stornvme,@stornvme.inf;%StorNVMe_ServiceDesc%;Microsoft
Standard NVM Express Driver,System32\drivers\stornvme.sys,Kernel driver,Boot Start,
Wed Mar 23 09:48:50 2016Z,BthHFEnum,@bthhfenum.inf;%BthHFEnum.SVCDESC%;Bluetooth
Hands-Free Audio and Call Control HID
Enumerator,\SystemRoot\System32\drivers\bthhfenum.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50
2016Z,BthHFSrv,@%SystemRoot%\System32\BthHFSrv.dll;-103,%SystemRoot%\System32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Wed Mar 23 09:48:50 2016Z,BthHFSrv\Parameters,,%SystemRoot%\System32\BthHFSrv.dll,,,
Wed Mar 23 09:48:50 2016Z,BTHPORT,@bth.inf;%BTHPORT.SvcDesc%;Bluetooth Port
Driver,\SystemRoot\System32\Drivers\BTHport.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50
2016Z,buttonconverter,@buttonconverter.inf;%btnconv.SvcDesc%;Service for Portable
Device Control devices,\SystemRoot\System32\drivers\buttonconverter.sys,Kernel
driver,Manual,
Wed Mar 23 09:48:50 2016Z,drmkaud,@wdmaudio.inf;%drmkaud.SvcDesc%;Microsoft Trusted
Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50 2016Z,msgpiowin32,@msgpiowin32.inf;%GPIO.SvcDesc%;Common Driver
for Buttons; DockMode and Laptop/Slate
Indicator,\SystemRoot\System32\drivers\msgpiowin32.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50 2016Z,sdbus,,\SystemRoot\System32\drivers\sdbus.sys,Kernel
driver,Manual,
Wed Mar 23 09:48:50 2016Z,usbehci,@usbport.inf;%EHCIMP.SvcDesc%;Microsoft USB 2.0
Enhanced Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbehci.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50 2016Z,usbhub,@usbport.inf;%ROOTHUB.SvcDesc%;Microsoft USB
Standard Hub Driver,\SystemRoot\System32\drivers\usbhub.sys,Kernel driver,Manual,
Wed Mar 23 09:48:50 2016Z,usbohci,@usbport.inf;%OHCIMP.SvcDesc%;Microsoft USB Open
Host Controller Miniport Driver,\SystemRoot\System32\drivers\usbohci.sys,Kernel
driver,Manual,
Wed Mar 23 09:48:50 2016Z,usbuhci,@usbport.inf;%UHCIMP.SvcDesc%;Microsoft USB
Universal Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbuhci.sys,Kernel driver,Manual,
Wed Mar 23 09:41:44 2016Z,BrYNSvc,BrYNSvc,"C:\Program Files
Page 134

SYSTEM OUTPUT.txt
(x86)\Browny02\BrYNSvc.exe",Own_Process,Manual,LocalSystem
Wed Mar 23 09:25:17
2016Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.ex
e -k imgsvc,Own_Process,Auto Start,NT Authority\LocalService
Tue Mar 22 13:52:39
2016Z,MsBridge,@%SystemRoot%\system32\bridgeres.dll;-1,System32\drivers\bridge.sys,K
ernel driver,Manual,
Tue Mar 22 13:52:38 2016Z,Ndisuio,NDIS Usermode I/O
Protocol,system32\drivers\ndisuio.sys,Kernel driver,Manual,
Tue Mar 22 13:52:38 2016Z,xboxgip,@xboxgip.inf;%XBOXGIP_Desc%;Xbox Game Input
Protocol Driver,\SystemRoot\System32\drivers\xboxgip.sys,Kernel driver,Manual,
Tue Mar 22 13:31:01 2016Z,CCDMonitorService,CCDMonitorService,C:\Program Files
(x86)\Acer\AOP Framework\CCDMonitorService.exe,Own_Process,Auto Start,LocalSystem
Tue Mar 22 13:31:00 2016Z,ose,Office Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",Own_Process,Manual,LocalSystem
Tue Mar 22 13:18:45
2016Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.ex
e -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Mar 22 13:16:27 2016Z,MSDTC Bridge 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,MSDTC Bridge 4.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,ServiceModelEndpoint 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,ServiceModelOperation 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,ServiceModelService 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,SMSvcHost 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,SMSvcHost 4.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,Windows Workflow Foundation 3.0.0.0,,,,,
Tue Mar 22 13:16:27 2016Z,Windows Workflow Foundation 4.0.0.0,,,,,
Tue Mar 22 13:15:54 2016Z,intaud_WaveExtensible,@oem8.inf;%INTAUD_WEX.SvcDesc%;Intel
WiDi Audio Device,\SystemRoot\system32\drivers\intelaud.sys,Kernel driver,Manual,
Tue Mar 22 13:15:48 2016Z,MSKSSRV,@ksfilter.inf;%MSKSSRV.DeviceDesc%;Microsoft
Streaming Service Proxy,\SystemRoot\system32\drivers\MSKSSRV.sys,Kernel
driver,Manual,
Tue Mar 22 13:15:48 2016Z,MSTEE,@ksfilter.inf;%MSTEE.DeviceDesc%;Microsoft Streaming
Tee/Sink-to-Sink Converter,\SystemRoot\system32\drivers\MSTEE.sys,Kernel
driver,Manual,
Tue Mar 22 13:15:31 2016Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
Service,%SystemRoot%\system32\igfxCUIService.exe,Own_Process,Auto Start,LocalSystem
Tue Mar 22 13:06:05 2016Z,iphlpsvc\Parameters,,%SystemRoot%\System32\iphlpsvc.dll,,,
Tue Mar 22 12:21:54
2016Z,EventLog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost
.exe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Mar 22 12:20:09 2016Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,
Tue Mar 22 11:54:41 2016Z,MBAMScheduler,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamscheduler.exe",Own_Process,Auto Start,LocalSystem
Tue Mar 22 11:54:39 2016Z,MBAMService,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamservice.exe",Own_Process,Auto Start,LocalSystem
Tue Mar 22 11:54:39
2016Z,MBAMWebAccessControl,,\??\C:\Windows\system32\drivers\mwac.sys,File system
driver,Manual,
Tue Mar 22 11:54:38
2016Z,MBAMProtector,,\??\C:\Windows\system32\drivers\mbam.sys,File system
driver,Manual,
Tue Mar 22 11:21:46 2016Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own_Process,Manual,LocalSystem
Tue Mar 22 10:37:21 2016Z,odserv,Microsoft Office Diagnostics Service,"C:\Program
Files (x86)\Common Files\Microsoft
Shared\OFFICE12\ODSERV.EXE",Own_Process,Manual,LocalSystem
Fri Sep 11 09:45:22
2015Z,WpdUpFltr,@%systemroot%\System32\drivers\WpdUpFltr.sys;-100,System32\drivers\W
pdUpFltr.sys,Kernel driver,Manual,
Fri Sep 11 09:45:22 2015Z,WUDFWpdFs,,\SystemRoot\system32\DRIVERS\WUDFRd.sys,Kernel
driver,Manual,\Driver\WudfRd
Page 135

SYSTEM OUTPUT.txt

Thu Aug 13 23:24:15
2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\SearchIndexer.exe /Embedding,Own_Process,Auto Start,LocalSystem
Thu Aug 13 23:03:20
2015Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,Own_Process,Manual,NT AUTHORITY\NetworkService
Thu Aug 13 22:52:11 2015Z,UcmUcsi,@ucmucsi.inf;%UcmUcsi.ServiceName%;USB Connector Manager UCSI Client,\SystemRoot\System32\drivers\UcmUcsi.sys,Kernel driver,Manual,
Thu Aug 13 22:37:27 2015Z,ePowerSvc,ePower Service,"C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe",Own_Process,Manual,LocalSystem
Thu Aug 13 22:35:41 2015Z,QALSvc,Quick Access Local Service,"C:\Program Files\Acer\Acer Quick Access\QALSvc.exe",Own_Process,Manual,NT AUTHORITY\LocalService
Thu Aug 13 22:35:41 2015Z,QASvc,Quick Access Service,"C:\Program Files\Acer\Acer Quick Access\QASvc.exe",Own_Process,Manual,LocalSystem
Thu Aug 13 22:34:01 2015Z,Dashlane Upgrade Service,,"C:\Program Files (x86)\Dashlane\Upgrade\DashlaneUpgradeService.exe",Own_Process,Auto Start,LocalSystem
Thu Aug 13 22:33:48 2015Z,Amazon 1Button App Service,Amazon 1Button App Service,"c:\Program Files (x86)\Amazon\Amazon1ButtonApp\Amazon1ButtonService64.Exe",Own_Process,Auto Start,LocalSystem
Thu Aug 13 22:25:21 2015Z,AtherosSvc,AtherosSvc,"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe",Own_Process,Auto Start,LocalSystem
Thu Aug 13 22:21:05 2015Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,
Thu Aug 13 22:19:13 2015Z,ICCS,Intel(R) Integrated Clock Controller Service - Intel(R) ICCS,"C:\Program Files (x86)\Intel\Intel(R) Integrated Clock Controller Service\ICCProxy.exe",Own_Process,Manual,LocalSystem
Thu Aug 13 22:19:11 2015Z,ialm,,,,,
Thu Aug 13 22:15:02 2015Z,Intel(R) Capability Licensing Service TCP IP Interface,Intel(R) Capability Licensing Service TCP IP Interface,"C:\Program Files\Intel\TXE Components\TCS\SocketHeciServer.exe",Own_Process,Manual,LocalSystem
Thu Aug 13 22:13:17
2015Z,HdAudAddService,@hdaudio.inf;%UAAFunctionDriverForHdAudio.SvcDesc%;Microsoft 1.1 UAA Function Driver for High Definition Audio Service,\SystemRoot\system32\DRIVERS\HdAudio.sys,Kernel driver,Manual,
Thu Aug 13 22:06:38 2015Z,ClipSVC\Parameters,,%SystemRoot%\System32\ClipSVC.dll,,,
Thu Aug 13 21:56:11
2015Z,WlanSvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Thu Aug 13 21:55:42 2015Z,acpipagr,@acpipagr.inf;%SvcDesc%;ACPI Processor Aggregator Driver,\SystemRoot\System32\drivers\acpipagr.sys,Kernel driver,Manual,
Thu Aug 13 21:55:42
2015Z,iaLPSSi_GPIO,@ialpssi_gpio.inf;%iaLPSSi_GPIO.SVCDESC%;Intel(R) Serial IO GPIO Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_GPIO.sys,Kernel driver,Manual,
Thu Aug 13 21:55:42
2015Z,iaLPSSi_I2C,@ialpssi_i2c.inf;%iaLPSSi_I2C.SVCDESC%;Intel(R) Serial IO I2C Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_I2C.sys,Kernel driver,Manual,
Thu Aug 13 21:55:42
2015Z,TPM,@tpm.inf;%TPM%;TPM,\SystemRoot\system32\drivers\tpm.sys,Kernel driver,Manual,
Thu Aug 13 21:54:58 2015Z,SecureLine,Avast SecureLine,C:\Program Files\AVAST Software\SecureLine\VpnSvc.exe,Own_Process,Auto Start,LocalSystem
Thu Aug 13 21:54:41 2015Z,3ware,,System32\drivers\3ware.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,ADP80XX,,System32\drivers\ADP80XX.SYS,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,agp440,@machine.inf;%agp440_svcdesc%;Intel AGP Bus Filter,System32\drivers\agp440.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,amdsata,,System32\drivers\amdsata.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,amdsbs,,System32\drivers\amdsbs.sys,Kernel driver,Boot

Page 136

SYSTEM OUTPUT.txt

Start,
Thu Aug 13 21:54:41 2015Z,amdxata,,System32\drivers\amdxata.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,arcsas,@arcsas.inf;%arcsas_ServiceName%;Adaptec
SAS/SATA-II RAID Storport's Miniport Driver,System32\drivers\arcsas.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,atapi,@mshdc.inf;%idechannel.DeviceDesc%;IDE
Channel,System32\drivers\atapi.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,b06bdrv,@netbvbda.inf;%vbd_srv_desc%;Broadcom NetXtreme II
VBD,System32\drivers\bxvbda.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,ebdrv,@netevbda.inf;%vbd_srv_desc%;QLogic 10 Gigabit
Ethernet Adapter VBD,System32\drivers\evbda.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41
2015Z,EhStorTcgDrv,@ehstortcgdrv.inf;%EhStorTcgDrv.Desc%;Microsoft driver for
storage devices supporting IEEE 1667 and TCG
protocols,System32\drivers\EhStorTcgDrv.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,gagp30kx,@machine.inf;%gagp30kx_svcdesc%;Microsoft Generic
AGPv3.0 Filter for K8 Processor Platforms,System32\drivers\gagp30kx.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,HpSAMD,,System32\drivers\HpSAMD.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,iaStorAV,@iastorav.inf;%iaStorAV.DeviceDesc%;Intel(R) SATA
RAID Controller Windows,System32\drivers\iaStorAV.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,iaStorV,@iastorv.inf;%*PNP0600.DeviceDesc%;Intel RAID
Controller Windows 7,System32\drivers\iaStorV.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,intelide,,System32\drivers\intelide.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,isapnp,,System32\drivers\isapnp.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS,,System32\drivers\lsi_sas.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS2i,,System32\drivers\lsi_sas2i.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS3i,,System32\drivers\lsi_sas3i.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SSS,,System32\drivers\lsi_sss.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,megasas,,System32\drivers\megasas.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,megasr,,System32\drivers\megasr.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,mvumis,,System32\drivers\mvumis.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,nvraid,,System32\drivers\nvraid.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,nvstor,,System32\drivers\nvstor.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,nv_agp,@machine.inf;%agpnvidia_svcdesc%;NVIDIA nForce AGP
Bus Filter,System32\drivers\nv_agp.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,pciide,,System32\drivers\pciide.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,pcmcia,,System32\drivers\pcmcia.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,percsas2i,,System32\drivers\percsas2i.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,percsas3i,,System32\drivers\percsas3i.sys,Kernel
driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,sbp2port,@sbp2.inf;%sbp2_ServiceDesc%;SBP-2
Transport/Protocol Bus Driver,System32\drivers\sbp2port.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,SiSRaid2,,System32\drivers\SiSRaid2.sys,Kernel driver,Boot
Start,
Thu Aug 13 21:54:41 2015Z,SiSRaid4,,System32\drivers\sisraid4.sys,Kernel driver,Boot

Page 137

SYSTEM OUTPUT.txt

Start,
Thu Aug 13 21:54:41 2015Z,stexstor,,System32\drivers\stexstor.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,storflt,@wstorflt.inf;%service_desc%;Microsoft Hyper-V Storage Accelerator,System32\drivers\vmstorfl.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,storufs,@storufs.inf;%UfsServiceDesc%;Microsoft Universal Flash Storage (UFS) Driver,System32\drivers\storufs.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,storvsc,,System32\drivers\storvsc.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,uagp35,@machine.inf;%uagp35_svcdesc%;Microsoft AGPv3.5 Filter,System32\drivers\uagp35.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,uliagpkx,@machine.inf;%uliagpkx_svcdesc%;Uli AGP Bus Filter,System32\drivers\uliagpkx.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,vmbus,@wvmbus.inf;%vmbus.SVCDESC%;Virtual Machine Bus,System32\drivers\vmbus.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,vsmraid,,System32\drivers\vsmraid.sys,Kernel driver,Boot Start,
Thu Aug 13 21:54:41 2015Z,VSTXRAID,@vstxraid.inf;%Driver.DeviceDesc%;VIA StorX Storage RAID Controller Windows Driver,System32\drivers\vstxraid.sys,Kernel driver,Boot Start,
Thu Jul 16 04:12:19 2015Z,WINUSB,@winusb.inf;%WINUSB_SvcDesc%;WinUsb Driver,\SystemRoot\System32\drivers\WinUSB.SYS,Kernel driver,Manual,
Thu Jul 16 04:12:16 2015Z,terminpt,@termmou.inf;%TermInpt.SVCDESC%;Microsoft Remote Desktop Input Driver,\SystemRoot\System32\drivers\terminpt.sys,Kernel driver,Manual,
Thu Jul 16 04:12:01 2015Z,kbdhid,@keyboard.inf;%KBDHID.SvcDesc%;Keyboard HID Driver,\SystemRoot\System32\drivers\kbdhid.sys,Kernel driver,Manual,
Thu Jul 16 04:11:59 2015Z,WUDFRd,@hidbthle.inf;%WudfRdDisplayName%;Windows Driver Foundation - User-mode Driver Framework Reflector,\SystemRoot\System32\drivers\WUDFRd.sys,Kernel driver,Manual,
Thu Jul 16 04:01:46 2015Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Thu Jul 16 03:47:02 2015Z,UEIPSvc,User Experience Improvement Program,"C:\Program Files\Acer\User Experience Improvement Program\Framework\UBTService.exe",Own_Process,Manual,LocalSystem
Thu Jul 16 03:46:19 2015Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe",Own_Process,Manual,LocalSystem
Thu Jul 16 03:44:48 2015Z,GamesAppIntegrationService,GamesAppIntegrationService,"C:\Program Files (x86)\WildTangent Games\App\GamesAppIntegrationService.exe",Own_Process,Auto Start,LocalSystem
Thu Jul 16 03:44:47 2015Z,GamesAppService,GamesAppService,"C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe",Own_Process,Manual,LocalSystem
Thu Jul 16 03:41:07 2015Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own_Process,Manual,NT Authority\LocalService
Thu Jul 16 03:40:55 2015Z,.NET CLR Data,,,,,
Thu Jul 16 03:40:55 2015Z,.NET CLR Networking,,,,,
Thu Jul 16 03:40:55 2015Z,clr_optimization_v2.0.50727_32,,,,,
Thu Jul 16 03:40:55 2015Z,clr_optimization_v2.0.50727_64,,,,,
Thu Jul 16 03:34:32 2015Z,PrintNotify,@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll;-1,%SystemRoot%\system32\svchost.exe -k print,288,Manual,LocalSystem
Thu Jul 16 03:34:32 2015Z,PrintNotify\Parameters,,C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll,,,
Thu Jul 16 03:32:47 2015Z,WlanSvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,
Thu Jul 16 03:32:44 2015Z,NativeWifiP,@%SystemRoot%\System32\drivers\nwifi.sys;-101,system32\DRIVERS\nwifi.sys,Kernel driver,Manual,
Thu Jul 16 03:31:44 2015Z,GPIOClx0101,Microsoft GPIO Class Extension
Page 138

SYSTEM OUTPUT.txt
Driver,System32\Drivers\msgpioclx.sys,Kernel driver,Manual,
Thu Jul 16 03:31:44 2015Z,SpbCx,Simple Peripheral Bus Support
Library,system32\drivers\SpbCx.sys,Kernel driver,Manual,
Fri Jul 10 13:19:52
2015Z,NgcCtnrSvc\Parameters,,%SystemRoot%\System32\NgcCtnrSvc.dll,,,
Fri Jul 10 13:19:52 2015Z,VaultSvc\Parameters,,C:\Windows\System32\vaultsvc.dll,,,
Fri Jul 10 13:14:47
2015Z,RDPDR,@%SystemRoot%\System32\DRIVERS\rdpdr.sys;-100,System32\drivers\rdpdr.sys
,Kernel driver,Manual,
Fri Jul 10 13:14:47 2015Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,Kernel driver,Manual,
Fri Jul 10 13:14:47
2015Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svcho
st.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 13:14:47
2015Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svch
ost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,localSystem
Fri Jul 10 13:14:46 2015Z,RDPUDD,,,,,
Fri Jul 10 13:14:46 2015Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,
Fri Jul 10 13:14:46
2015Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,
Fri Jul 10 12:22:48
2015Z,Synth3dVsc,,\SystemRoot\System32\drivers\Synth3dVsc.sys,Kernel driver,Manual,
Fri Jul 10 12:22:47 2015Z,dmvsc,,\SystemRoot\System32\drivers\dmvsc.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:47 2015Z,gencounter,@wgencounter.inf;%GenCounter.SVCDESC%;Microsoft
Hyper-V Generation Counter,\SystemRoot\System32\drivers\vmgencounter.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:44 2015Z,UASPStor,@uaspstor.inf;%UASPortName%;USB Attached SCSI
(UAS) Driver,\SystemRoot\System32\drivers\uaspstor.sys,Kernel driver,Manual,
Fri Jul 10 12:22:43 2015Z,sdstor,@sdstor.inf;%sdstor_ServiceDesc%;SD Storage Port
Driver,\SystemRoot\System32\drivers\sdstor.sys,Kernel driver,Manual,
Fri Jul 10 12:22:41 2015Z,npsvctrig,@npsvctrig.inf;%NPSVCTRIG.SvcDisplayName%;Named
pipe service trigger provider,\SystemRoot\System32\drivers\npsvctrig.sys,Kernel
driver,System Start,
Fri Jul 10 12:22:39
2015Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,\SystemRoot\System32\drivers
\asyncmac.sys,Kernel driver,Manual,
Fri Jul 10 12:22:25 2015Z,IPMIDRV,,\SystemRoot\System32\drivers\IPMIDrv.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:25 2015Z,iScsiPrt,@iscsi.inf;%iScsiPortName%;iScsiPort
Driver,\SystemRoot\System32\drivers\msiscsi.sys,Kernel driver,Manual,
Fri Jul 10 12:22:22 2015Z,HidBatt,@hidbatt.inf;%HidBatt.SvcDesc%;HID UPS Battery
Driver,\SystemRoot\System32\drivers\HidBatt.sys,Kernel driver,Manual,
Fri Jul 10 12:22:22
2015Z,mshidumdf,@%SystemRoot%\system32\drivers\mshidumdf.sys;-100,\SystemRoot\System
32\drivers\mshidumdf.sys,Kernel driver,Manual,
Fri Jul 10 12:22:21 2015Z,fdc,@fdc.inf;%fdc_ServiceDesc%;Floppy Disk Controller
Driver,\SystemRoot\System32\drivers\fdc.sys,Kernel driver,Manual,
Fri Jul 10 12:22:21 2015Z,flpydisk,@flpydisk.inf;%floppy_ServiceDesc%;Floppy Disk
Driver,\SystemRoot\System32\drivers\flpydisk.sys,Kernel driver,Manual,
Fri Jul 10 12:22:21 2015Z,sfloppy,@flpydisk.inf;%sfloppy_devdesc%;High-Capacity
Floppy Disk Drive,\SystemRoot\System32\drivers\sfloppy.sys,Kernel driver,Manual,
Fri Jul 10 12:22:20 2015Z,CapImg,@capimg.inf;%CapImgHid_Service%;HID driver for
CapImg touch screen,\SystemRoot\System32\drivers\capimg.sys,Kernel driver,Manual,
Fri Jul 10 12:22:19 2015Z,BTHMODEM,@bthspp.inf;%BthSerial.DisplayName%;Bluetooth
Serial Communications Driver,\SystemRoot\System32\drivers\bthmodem.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:18 2015Z,bthhfhid,@bthaudhid.inf;%BthAudioHFHid.SVCDESC%;Bluetooth
Hands-Free Call Control HID,\SystemRoot\System32\drivers\BthHFHid.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:16 2015Z,1394ohci,@1394.inf;%PCI\CC_0C0010.DeviceDesc%;1394 OHCI
Page 139

SYSTEM OUTPUT.txt
Compliant Host Controller,\SystemRoot\System32\drivers\1394ohci.sys,Kernel
driver,Manual,
Fri Jul 10 12:22:16 2015Z,AcpiPmi,@acpipmi.inf;%AcpiPmi.SvcDesc%;ACPI Power Meter
Driver,\SystemRoot\System32\drivers\acpipmi.sys,Kernel driver,Manual,
Fri Jul 10 12:22:08
2015Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost
.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 12:21:44
2015Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchos
t.exe -k NetSvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 12:21:44
2015Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 12:21:43 2015Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel
driver,Auto Start,
Fri Jul 10 12:21:43 2015Z,srvnet,,System32\DRIVERS\srvnet.sys,File system
driver,Manual,
Fri Jul 10 12:21:42
2015Z,MsLldp,@%SystemRoot%\system32\drivers\mslldp.sys;-200,system32\drivers\mslldp.
sys,Kernel driver,Auto Start,
Fri Jul 10 12:21:37 2015Z,crypt32,,,,,
Fri Jul 10 12:21:24 2015Z,hyperkbd,,\SystemRoot\System32\drivers\hyperkbd.sys,Kernel
driver,Manual,
Fri Jul 10 12:21:24
2015Z,HyperVideo,,\SystemRoot\system32\DRIVERS\HyperVideo.sys,Kernel driver,Manual,
Fri Jul 10 12:21:24 2015Z,netvsc,,\SystemRoot\System32\drivers\netvsc.sys,Kernel
driver,Manual,
Fri Jul 10 12:21:24 2015Z,s3cap,,\SystemRoot\System32\drivers\vms3cap.sys,Kernel
driver,Manual,
Fri Jul 10 12:21:24 2015Z,VMBusHID,,\SystemRoot\System32\drivers\VMBusHID.sys,Kernel
driver,Manual,
Fri Jul 10 12:21:21
2015Z,cnghwassist,@%SystemRoot%\system32\drivers\cnghwassist.sys;-100,System32\DRIVE
RS\cnghwassist.sys,Kernel driver,Disabled,
Fri Jul 10 12:20:51 2015Z,NETVSCVFPP,,,,,
Fri Jul 10 12:20:44
2015Z,NetSetupSvc,@%SystemRoot%\system32\NetSetupSvc.dll;-3,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 12:20:30
2015Z,Psched,@%windir%\System32\drivers\pacer.sys;-101,System32\drivers\pacer.sys,Ke
rnel driver,System Start,
Fri Jul 10 12:20:30
2015Z,vwififlt,@%SystemRoot%\System32\drivers\vwififlt.sys;-259,System32\drivers\vwi
fiflt.sys,Kernel driver,System Start,
Fri Jul 10 12:20:26
2015Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Ke
rnel driver,Boot Start,
Fri Jul 10 12:20:26 2015Z,Tcpip6,@todo.dll;-100;Microsoft IPv6 Protocol
Driver,System32\drivers\tcpip.sys,Kernel driver,Manual,
Fri Jul 10 12:20:26 2015Z,TCPIP6TUNNEL,,,,,
Fri Jul 10 12:20:26 2015Z,TCPIPTUNNEL,,,,,
Fri Jul 10 12:20:26
2015Z,WFPLWFS,@%SystemRoot%\System32\drivers\wfplwfs.sys;-6000,System32\drivers\wfpl
wfs.sys,Kernel driver,Boot Start,
Fri Jul 10 12:20:23 2015Z,acpiex,Microsoft ACPIEX
Driver,System32\Drivers\acpiex.sys,Kernel driver,Boot Start,
Fri Jul 10 12:20:23 2015Z,Ucx01000,USB Host Support
Library,system32\drivers\ucx01000.sys,Kernel driver,Manual,
Fri Jul 10 12:20:23 2015Z,WindowsTrustedRT,Windows Trusted Execution Environment
Class Extension,system32\drivers\WindowsTrustedRT.sys,Kernel driver,Boot Start,
Fri Jul 10 12:20:23
2015Z,WindowsTrustedRTProxy,@WindowsTrustedRTProxy.inf;%WindowsTrustedRTProxy.SVCDES
C%;Microsoft Windows Trusted Runtime Secure
Page 140

SYSTEM OUTPUT.txt

Service,System32\drivers\WindowsTrustedRTProxy.sys,Kernel driver,Boot Start,
Fri Jul 10 11:06:22
2015Z,AudioEndpointBuilder,@%SystemRoot%\system32\AudioEndpointBuilder.dll;-204,%Sys
temRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem
Fri Jul 10 11:06:22
2015Z,Audiosrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Fri Jul 10 11:06:22
2015Z,MMCSS,@%systemroot%\system32\drivers\mmcss.sys;-100,\SystemRoot\system32\drive
rs\mmcss.sys,Kernel driver,Auto Start,
Fri Jul 10 11:06:01 2015Z,Winsock,,,,,
Fri Jul 10 11:05:46
2015Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32
\svchost.exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:46
2015Z,NdisImPlatform,@%SystemRoot%\System32\drivers\ndisimplatform.sys;-501,System32
\drivers\NdisImPlatform.sys,Kernel driver,Manual,
Fri Jul 10 11:05:46
2015Z,NetBIOS,@%windir%\system32\drivers\netbios.sys;-503,system32\drivers\netbios.s
ys,File system driver,System Start,
Fri Jul 10 11:05:46 2015Z,NetbiosSmb,,,,,
Fri Jul 10 11:05:46 2015Z,RDMANDK,,,,,
Fri Jul 10 11:05:25
2015Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\
afd.sys,Kernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,ahcache,@%systemroot%\system32\drivers\ahcache.sys;-102,system32\DRIVERS\ahcac
he.sys,Kernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,AJRouter,@%SystemRoot%\system32\AJRouter.dll;-2,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own_Proc
ess,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,AppID,@%systemroot%\system32\srpapi.dll;-100,\SystemRoot\system32\drivers\appi
d.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
Authority\LocalService
Fri Jul 10 11:05:25
2015Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,AppReadiness,@%SystemRoot%\System32\AppReadiness.dll;-1000,%SystemRoot%\System
32\svchost.exe -k AppReadiness,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,AppXSvc,@%SystemRoot%\system32\appxdeploymentserver.dll;-1,%systemroot%\system
32\svchost.exe -k wsappx,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchos
t.exe -k AxInstSVGroup,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25 2015Z,Beep,Beep,,Kernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25

Page 141

SYSTEM OUTPUT.txt
2015Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,Fil
e system driver,Manual,
Fri Jul 10 11:05:25
2015Z,BrokerInfrastructure,@%windir%\system32\bisrv.dll;-100,%SystemRoot%\system32\s
vchost.exe -k DcomLaunch,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.
exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,File system driver,Disabled,
Fri Jul 10 11:05:25
2015Z,CDPSvc,@%SystemRoot%\system32\cdpsvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,CLFS,@%SystemRoot%\system32\drivers\clfs.sys;-100,System32\drivers\CLFS.sys,Ke
rnel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,ClipSVC,@%SystemRoot%\system32\ClipSVC.dll;-103,%SystemRoot%\System32\svchost.
exe -k wsappx,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,condrv,Console Driver,System32\drivers\condrv.sys,Kernel
driver,Manual,
Fri Jul 10 11:05:25
2015Z,CoreMessagingRegistrar,@%SystemRoot%\system32\coremessaging.dll;-1,%SystemRoot
%\system32\svchost.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k NetworkService,Share_Process,Auto Start,NT Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,dam,@%SystemRoot%\system32\drivers\dam.sys;-100,system32\drivers\dam.sys,Kerne
l driver,System Start,
Fri Jul 10 11:05:25
2015Z,DcomLaunch,@combase.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,DcpSvc,@%SystemRoot%\system32\dcpsvc.dll;-3001,%SystemRoot%\System32\svchost.e
xe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svch
ost.exe -k defragsvc,Own_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,DeviceInstall,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\s
vchost.exe -k DcomLaunch,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,DevQueryBroker,@%SystemRoot%\system32\DevQueryBroker.dll;-100,%SystemRoot%\sys
tem32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,Dfsc,@%systemroot%\system32\wkssvc.dll;-1008,System32\Drivers\dfsc.sys,File
system driver,System Start,
Fri Jul 10 11:05:25
2015Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService
Page 142

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,diagnosticshub.standardcollector.service,@%SystemRoot%\system32\DiagSvcs\Diagn
osticsHub.StandardCollector.ServiceRes.dll;-1000,%SystemRoot%\system32\DiagSvcs\Diag
nosticsHub.StandardCollector.Service.exe,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,DiagTrack,@%SystemRoot%\system32\diagtrack.dll;-3001,%SystemRoot%\System32\svc
host.exe -k utcsvc,Own_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,DmEnrollmentSvc,@%systemroot%\system32\Windows.Internal.Management.dll;-100,%s
ystemroot%\system32\svchost.exe -k netsvcs,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,dmwappushservice,@%SystemRoot%\System32\dmwappushsvc.dll;-200,%SystemRoot%\sys
tem32\svchost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,DoSvc,@%systemroot%\system32\dosvc.dll;-100,%systemroot%\system32\svchost.exe
-k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,DsmSvc,@%SystemRoot%\system32\DeviceSetupManager.dll;-1000,%SystemRoot%\system
32\svchost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,DsSvc,@%SystemRoot%\system32\dssvc.dll;-10003,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,Eaphost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Sha
re_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,embeddedmode,@%SystemRoot%\system32\embeddedmodesvc.dll;-200,%SystemRoot%\Syst
em32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,EntAppSvc,@EnterpriseAppMgmtSvc.dll;-1,%systemroot%\system32\svchost.exe -k
appmodel,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,exfat,exFAT File System Driver,,File system driver,Manual,
Fri Jul 10 11:05:25 2015Z,fastfat,FAT12/16/32 File System Driver,,File system
driver,Manual,
Fri Jul 10 11:05:25
2015Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,O
wn_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,fhsvc,@%systemroot%\system32\fhsvc.dll;-101,%SystemRoot%\system32\svchost.exe
Page 143

SYSTEM OUTPUT.txt
-k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,FileCrypt,@%systemroot%\system32\drivers\filecrypt.sys;-100,system32\drivers\f
ilecrypt.sys,File system driver,System Start,
Fri Jul 10 11:05:25
2015Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,System32\drivers\fil
einfo.sys,File system driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmg
r.sys,File system driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho
st.exe -k LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers
\FsDepends.sys,File system driver,Manual,
Fri Jul 10 11:05:25 2015Z,Fs_Rec,,,8,Boot Start,
Fri Jul 10 11:05:25 2015Z,gpsvc,@gpapi.dll;-112,%systemroot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,GpuEnergyDrv,@%SystemRoot%\system32\drivers\gpuenergydrv.sys;-100,System32\dri
vers\gpuenergydrv.sys,Kernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,Kern
el driver,Manual,
Fri Jul 10 11:05:25
2015Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwp
olicy.sys,Kernel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,icssvc,@%SystemRoot%\System32\tetheringservice.dll;-4097,%SystemRoot%\system32
\svchost.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
Authority\LocalService
Fri Jul 10 11:05:25
2015Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%Syst
emRoot%\system32\IEEtwCollector.exe /V,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,IoQos,@%SystemRoot%\system32\drivers\ioqos.sys;-100,system32\drivers\ioqos.sys
,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt
drv.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.
sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share_Process,Manual,L
ocalSystem
Fri Jul 10 11:05:25 2015Z,KSecDD,,System32\Drivers\ksecdd.sys,Kernel driver,Boot
Page 144

SYSTEM OUTPUT.txt
Start,
Fri Jul 10 11:05:25 2015Z,KSecPkg,,System32\Drivers\ksecpkg.sys,Kernel driver,Boot
Start,
Fri Jul 10 11:05:25 2015Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,lfsvc,@%SystemRoot%\System32\lfsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,LicenseManager,@%SystemRoot%\system32\licensemanagersvc.dll;-200,%SystemRoot%\
System32\svchost.exe -k LocalService,Share_Process,Manual,NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.ex
e -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\System32\svchost.e
xe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,LSM,@%windir%\system32\lsm.dll;-1001,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drive
rs\luafv.sys,File system driver,Auto Start,
Fri Jul 10 11:05:25
2015Z,MapsBroker,@%SystemRoot%\System32\moshost.dll;-100,%SystemRoot%\System32\svcho
st.exe -k NetworkService,Own_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,Modem,,system32\drivers\modem.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mou
ntmgr.sys,Kernel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,mpsdrv,@%SystemRoot%\system32\drivers\mpsdrv.sys;-23092,System32\drivers\mpsdr
v.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svc
host.exe -k LocalServiceNoNetwork,Share_Process,Auto Start,NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mr
xdav.sys,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,Fil
e system driver,Manual,
Fri Jul 10 11:05:25
2015Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys
,File system driver,Auto Start,
Fri Jul 10 11:05:25
2015Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys
,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchos
t.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.
exe /V,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,File
system driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,NcaSvc,@%SystemRoot%\system32\ncasvc.dll;-3009,%SystemRoot%\System32\svchost.e
xe -k NetSvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,NcbService,@%SystemRoot%\system32\ncbservice.dll;-500,%SystemRoot%\System32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Page 145

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,NcdAutoSetup,@%SystemRoot%\system32\NcdAutoSetup.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalServiceNoNetwork,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Ke
rnel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,NdisCap,@%SystemRoot%\System32\drivers\ndiscap.sys;-5000,System32\drivers\ndis
cap.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,Ndu,@%SystemRoot%\system32\drivers\Ndu.sys;-10001,system32\drivers\Ndu.sys,Ker
nel driver,Auto Start,
Fri Jul 10 11:05:25
2015Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,K
ernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.
exe,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,netprofm,@%SystemRoot%\system32\netprofmsvc.dll;-202,%SystemRoot%\System32\svc
host.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NetTcpPortSharing,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceMo
delInstallRC.dll;-8201,%systemroot%\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.e
xe,Share_Process,Disabled,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NgcCtnrSvc,@%SystemRoot%\System32\NgcCtnrSvc.dll;-1,%SystemRoot%\system32\svch
ost.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NgcSvc,@%SystemRoot%\System32\ngcsvc.dll;-100,%SystemRoot%\system32\lsass.exe,
Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,Share_Process,Auto Start,NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsipr
oxy.sys,Kernel driver,System Start,
Fri Jul 10 11:05:25 2015Z,NTFS,,,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,OneSyncSvc,@%SystemRoot%\system32\APHostRes.dll;-10002,%SystemRoot%\system32\s
vchost.exe -k UnistackSvcGroup,96,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25 2015Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,Kernel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,pdc,@%SystemRoot%\system32\drivers\pdc.sys;-100,system32\drivers\pdc.sys,Kerne
l driver,Boot Start,

Page 146

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,PerfHost,@%systemroot%\sysWow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PimIndexMaintenanceSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-15001,%Sy
stemRoot%\system32\svchost.exe -k UnistackSvcGroup,96,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-200,%SystemRoot%\system32\svchos
t.exe -k DcomLaunch,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\sv
chost.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost
.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\sv
chost.exe -k NetworkServiceNetworkRestricted,Share_Process,Manual,NT
Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\d
rivers\qwavedrv.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
xe -k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File
system driver,System Start,
Fri Jul 10 11:05:25 2015Z,ReFSv1,,,File system driver,Manual,
Fri Jul 10 11:05:25
2015Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,Share_Process,Disabled,localSystem
Fri Jul 10 11:05:25
2015Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
localService,Share_Process,Disabled,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,RetailDemo,@%SystemRoot%\System32\RDXService.dll;-256,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator
.exe,Own_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,RpcSs,@combase.dll;-5010,%SystemRoot%\system32\svchost.exe
-k rpcss,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Sha

Page 147

SYSTEM OUTPUT.txt
re_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,Share_Process,Disabled,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,ScDeviceEnum,@%SystemRoot%\System32\ScDeviceEnum.dll;-100,%SystemRoot%\system3
2\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfi
lter.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.ex
e -k SDRSVC,Own_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.e
xe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,SensorDataService,@%SystemRoot%\system32\SensorDataService.exe;-101,%SystemRoo
t%\System32\SensorDataService.exe,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,SensorService,@%SystemRoot%\System32\sensorservice.dll;-1000,%SystemRoot%\syst
em32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,SerCx,Serial UART Support
Library,system32\drivers\SerCx.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,SerCx2,Serial UART Support
Library,system32\drivers\SerCx2.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svch
ost.exe -k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\sv
chost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System3
2\svchost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,smphost,@%SystemRoot%\System32\smphost.dll;-102,%SystemRoot%\System32\svchost.
exe -k smphost,Own_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,SmsRouter,@%SystemRoot%\System32\SmsRouterSvc.dll;-10001,%SystemRoot%\system32
\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap
.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.ex
e,272,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe
,Own_Process,Auto Start,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,File
system driver,Auto Start,

Page 148

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,File
system driver,Manual,
Fri Jul 10 11:05:25
2015Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.
exe.-k LocalService,Share_Process,Manual,NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,StateRepository,@%SystemRoot%\system32\windows.staterepository.dll;-1,%SystemR
oot%\system32\svchost.exe -k appmodel,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,storqosflt,@%SystemRoot%\System32\drivers\storqosflt.sys;-101,system32\drivers
\storqosflt.sys,File system driver,Auto Start,
Fri Jul 10 11:05:25
2015Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.
exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,svsvc,@%SystemRoot%\system32\svsvc.dll;-101,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe
-k swprv,Own_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,SystemEventsBroker,@%windir%\system32\SystemEventsBrokerServer.dll;-1001,%Syst
emRoot%\system32\svchost.exe -k DcomLaunch,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchos
t.exe -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,
Fri Jul 10 11:05:25
2015Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,\SystemRoot\system32\DRIVERS\td
x.sys,Kernel driver,System Start,
Fri Jul 10 11:05:25
2015Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,Share_Process,Manual,NT Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
host.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,tiledatamodelsvc,@%SystemRoot%\system32\tileobjserver.dll;-1,%systemroot%\syst
em32\svchost.exe -k appmodel,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,TimeBroker,@%windir%\system32\TimeBrokerServer.dll;-1001,%SystemRoot%\system32
\svchost.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,TrkWks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,TsUsbFlt,@%SystemRoot%\system32\drivers\tsusbflt.sys;-1000,System32\drivers\Ts
UsbFlt.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,UcmCx0101,USB Connector Manager KMDF Class
Extension,System32\Drivers\UcmCx.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,UdeCx,USB Device Emulation Support
Library,system32\drivers\udecx.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,udfs,udfs,system32\DRIVERS\udfs.sys,File system
driver,Disabled,

Page 149

SYSTEM OUTPUT.txt

```
Fri Jul 10 11:05:25 2015Z,Ufx01000,USB Function Class
Extension,system32\drivers\ufx01000.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,UIODetect,@%SystemRoot%\system32\ui0detect.exe;-101,%SystemRoot%\system32\UIOD
etect.exe,272,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,UnistoreSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-10003,%SystemRoot%\S
ystem32\svchost.exe -k UnistackSvcGroup,96,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,UrsCx01000,USB Role-Switch Support
Library,system32\drivers\urscx01000.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,UserDataSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-14001,%SystemRoot%\s
ystem32\svchost.exe -k UnistackSvcGroup,96,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,UserManager,@%systemroot%\system32\usermgr.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Fri Jul 10 11:05:25
2015Z,UsoSvc,@%systemroot%\system32\usocore.dll;-102,%systemroot%\system32\svchost.e
xe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Proc
ess,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vhf,@%SystemRoot%\system32\drivers\vhf.sys;-100,\SystemRoot\System32\drivers\v
hf.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,vmicguestinterface,@%systemroot%\system32\icsvc.dll;-801,%systemroot%\system32
\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicheartbeat,@%systemroot%\system32\icsvc.dll;-101,%systemroot%\system32\svch
ost.exe -k ICService,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmickvpexchange,@%systemroot%\system32\icsvc.dll;-201,%systemroot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicrdv,@%systemroot%\system32\icsvc.dll;-601,%systemroot%\system32\svchost.ex
e -k ICService,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicshutdown,@%systemroot%\system32\icsvc.dll;-301,%systemroot%\system32\svcho
st.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmictimesync,@%systemroot%\system32\icsvc.dll;-401,%systemroot%\system32\svcho
st.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,vmicvmsession,@%systemroot%\system32\icsvc.dll;-901,%systemroot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicvss,@%systemroot%\system32\icsvc.dll;-501,%systemroot%\system32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmg
rx.sys,Kernel driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_
Process,Manual,LocalSystem
```

Page 150

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WalletService,@%SystemRoot%\System32\WalletService.dll;-1000,%SystemRoot%\Syst
em32\svchost.exe -k appmodel,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",Own_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k WbioSvcGroup,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,Wcmsvc,@%SystemRoot%\System32\wcmsvc.dll;-4097,%SystemRoot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService
Fri Jul 10 11:05:25
2015Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcssvc,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,wdiwifi,WDI Driver
Framework,system32\DRIVERS\wdiwifi.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25 2015Z,WdNisSvc,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-320,"%ProgramFiles%\Windows
Defender\NisSrv.exe",Own_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,WEPHOSTSVC,@%systemroot%\system32\wephostsvc.dll;-100,%systemroot%\system32\sv
chost.exe -k WepHostSvcGroup,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,Share_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,Own_Process,Manual,localSystem
Fri Jul 10 11:05:25
2015Z,WiaRpc,@%SystemRoot%\system32\wiarpc.dll;-2,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25 2015Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,File
system driver,Manual,
Fri Jul 10 11:05:25
2015Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,localSystem
Fri Jul 10 11:05:25
2015Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25

Page 151

SYSTEM OUTPUT.txt
2015Z,wlidsvc,@%SystemRoot%\system32\wlidsvc.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,Own_Process,Manual,localSystem
Fri Jul 10 11:05:25 2015Z,WMPNetworkSvc,@%PROGRAMFILES%\windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\windows Media
Player\wmpnetwk.exe",Own_Process,Manual,NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,Wof,Windows Overlay File System Filter Driver,,File system
driver,Boot Start,
Fri Jul 10 11:05:25
2015Z,workfolderssvc,@%systemroot%\system32\workfolderssvc.dll;-102,%SystemRoot%\Sys
tem32\svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,wpcfltr,Family Safety Filter
Driver,system32\DRIVERS\wpcfltr.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,WpnService,@%SystemRoot%\system32\wpnservice.dll;-1,%systemroot%\system32\svch
ost.exe -k wswpnservice,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\
drivers\ws2ifsl.sys,Kernel driver,Disabled,
Fri Jul 10 11:05:25
2015Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WSService,@%SystemRoot%\system32\WSService.dll;-103,%SystemRoot%\System32\svch
ost.exe -k wsappx,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,WudfPf,@%SystemRoot%\system32\drivers\wudfpf.sys;-1000,system32\drivers\WudfPf
.sys,Kernel driver,Manual,
Fri Jul 10 11:05:25
2015Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalServiceNoNetwork,Share_Process,Manual,NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,XblAuthManager,@%systemroot%\system32\XblAuthManager.dll;-100,%SystemRoot%\sys
tem32\svchost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,XblGameSave,@%systemroot%\system32\XblGameSave.dll;-100,%SystemRoot%\system32\
svchost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:25
2015Z,XboxNetApiSvc,@%systemroot%\system32\XboxNetApiSvc.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k netsvcs,Share_Process,Manual,LocalSystem
Fri Jul 10 11:05:06 2015Z,.NET CLR Networking 4.0.0.0,,,,,,
Fri Jul 10 11:05:06 2015Z,.NET Data Provider for Oracle,,,,,,
Fri Jul 10 11:05:06 2015Z,.NET Data Provider for SqlServer,,,,,,
Fri Jul 10 11:05:06 2015Z,.NET Memory Cache 4.0,,,,,,
Fri Jul 10 11:05:06 2015Z,.NETFramework,,,,,
Fri Jul 10 11:05:06 2015Z,ADOVMPPackage,,,,,
Fri Jul 10 11:05:06 2015Z,adsi,,,,,,
Fri Jul 10 11:05:06 2015Z,AJRouter\Parameters,,%SystemRoot%\System32\AJRouter.dll,,,
Fri Jul 10 11:05:06 2015Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,
Fri Jul 10 11:05:06
2015Z,AppReadiness\Parameters,,%SystemRoot%\system32\AppReadiness.dll,,,
Fri Jul 10 11:05:06
2015Z,AppXSvc\Parameters,,%SystemRoot%\system32\appxdeploymentserver.dll,,,
Page 152

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:06 2015Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\AudioEndpointBuilder.dl
l,;,;
Fri Jul 10 11:05:06 2015Z,Audiosrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Fri Jul 10 11:05:06 2015Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,
Fri Jul 10 11:05:06 2015Z,BattC,;,,
Fri Jul 10 11:05:06 2015Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,
Fri Jul 10 11:05:06 2015Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,
Fri Jul 10 11:05:06 2015Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Fri Jul 10 11:05:06 2015Z,BrokerInfrastructure\Parameters,,%SystemRoot%\System32\bisrv.dll,,,
Fri Jul 10 11:05:06 2015Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,
Fri Jul 10 11:05:06 2015Z,CDPSvc\Parameters,,%SystemRoot%\System32\CDPSvc.dll,,,
Fri Jul 10 11:05:06 2015Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Fri Jul 10 11:05:06 2015Z,clr_optimization_v4.0.30319_32,,,,
Fri Jul 10 11:05:06 2015Z,clr_optimization_v4.0.30319_64,,,,
Fri Jul 10 11:05:06 2015Z,CoreMessagingRegistrar\Parameters,,%SystemRoot%\system32\coremessaging.dll,,,
Fri Jul 10 11:05:06 2015Z,CoreUI,;,;
Fri Jul 10 11:05:06 2015Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,DCLocator,;,,
Fri Jul 10 11:05:06 2015Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Fri Jul 10 11:05:06 2015Z,DcpSvc\Parameters,,%SystemRoot%\system32\dcpsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,DeviceAssociationService\Parameters,,%SystemRoot%\system32\das.dll,,,
Fri Jul 10 11:05:06 2015Z,DevQueryBroker\Parameters,,%SystemRoot%\system32\DevQueryBroker.dll,,,
Fri Jul 10 11:05:06 2015Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,
Fri Jul 10 11:05:06 2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,
Fri Jul 10 11:05:06 2015Z,DmEnrollmentSvc\Parameters,,%Systemroot%\system32\Windows.Internal.Management.
dll,;,;
Fri Jul 10 11:05:06 2015Z,dmwappushservice\Parameters,,%SystemRoot%\system32\dmwappushsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,
Fri Jul 10 11:05:06 2015Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,
Fri Jul 10 11:05:06 2015Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Fri Jul 10 11:05:06 2015Z,DsmSvc\Parameters,,%SystemRoot%\System32\DeviceSetupManager.dll,,,
Fri Jul 10 11:05:06 2015Z,DsSvc\Parameters,,%SystemRoot%\System32\DsSvc.dll
Fri Jul 10 11:05:06 2015Z,Eaphost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,EFS\Parameters,,%SystemRoot%\system32\efssvc.dll,,,
Fri Jul 10 11:05:06 2015Z,embeddedmode\Parameters,,%SystemRoot%\System32\embeddedmodesvc.dll,,,
Fri Jul 10 11:05:06 2015Z,EntAppSvc\Parameters,,%SystemRoot%\system32\EnterpriseAppMgmtSvc.dll,,,
Fri Jul 10 11:05:06 2015Z,ESENT,,,,
Fri Jul 10 11:05:05 2015Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,
Fri Jul 10 11:05:05 2015Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,
Fri Jul 10 11:05:05 2015Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,
Fri Jul 10 11:05:05 2015Z,fhsvc\Parameters,,%SystemRoot%\system32\fhsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,;
Fri Jul 10 11:05:05 2015Z,gpsvc\Parameters,,%SystemRoot%\system32\gpsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,
Fri Jul 10 11:05:05 2015Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,

Page 153

SYSTEM OUTPUT.txt

```
Fri Jul 10 11:05:05 2015Z,icssvc\Parameters,,%SystemRoot%\System32\tetheringservice.dll,;,;
Fri Jul 10 11:05:05 2015Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,
Fri Jul 10 11:05:05 2015Z,inetaccs,,,,,
Fri Jul 10 11:05:05 2015Z,KeyIso\Parameters,,%SystemRoot%\system32\keyiso.dll,,,
Fri Jul 10 11:05:05 2015Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,
Fri Jul 10 11:05:05 2015Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Fri Jul 10 11:05:05 2015Z,ldap,,,;
Fri Jul 10 11:05:05 2015Z,lfsvc\Parameters,,%SystemRoot%\System32\lfsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,LicenseManager\Parameters,,%SystemRoot%\system32\LicenseManagerSvc.dll,
Fri Jul 10 11:05:05 2015Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Lsa,,,,
Fri Jul 10 11:05:05 2015Z,LSM\Parameters,,%SystemRoot%\System32\lsm.dll,,,
Fri Jul 10 11:05:05 2015Z,MapsBroker\Parameters,,%SystemRoot%\System32\moshost.dll,,;,
Fri Jul 10 11:05:05 2015Z,Mpssvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Msfs,,,File system driver,System Start,
Fri Jul 10 11:05:05 2015Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,
Fri Jul 10 11:05:05 2015Z,MsRPC,,,Kernel driver,Manual,
Fri Jul 10 11:05:05 2015Z,MSSCNTRS,,,,,
Fri Jul 10 11:05:05 2015Z,napagent,,,,;
Fri Jul 10 11:05:05 2015Z,Ncasvc\Parameters,,%SystemRoot%\System32\ncasvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Ncbservice\Parameters,,%SystemRoot%\System32\ncbservice.dll,,,
Fri Jul 10 11:05:05 2015Z,NcdAutosetup\Parameters,,%SystemRoot%\System32\NcdAutoSetup.dll,,;,
Fri Jul 10 11:05:05 2015Z,Netlogon\Parameters,,%SystemRoot%\system32\netlogon.dll,,,
Fri Jul 10 11:05:05 2015Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,
Fri Jul 10 11:05:05 2015Z,netprofm\Parameters,,%SystemRoot%\System32\netprofmsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NetSetupSvc\Parameters,,%SystemRoot%\System32\NetSetupSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NgcSvc\Parameters,,%SystemRoot%\system32\ngcsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Npfs,,,File system driver,System Start,
Fri Jul 10 11:05:05 2015Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NTDS,,,,;
Fri Jul 10 11:05:05 2015Z,Null,,,,Kernel driver,System Start, .
Fri Jul 10 11:05:05 2015Z,OneSyncSvc\Parameters,,%SystemRoot%\System32\APHostService.dll,,,
Fri Jul 10 11:05:05 2015Z,p2pimsvc\Parameters,,%SystemRoot%\System32\pnrpsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,p2psvc\Parameters,,%SystemRoot%\System32\p2psvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PerfDisk,,,,,
Fri Jul 10 11:05:05 2015Z,PerfNet,,,,,
Fri Jul 10 11:05:05 2015Z,PerfOS,,,,,
Fri Jul 10 11:05:05 2015Z,PerfProc,,,,,;
Fri Jul 10 11:05:05 2015Z,PimIndexMaintenanceSvc\Parameters,,%SystemRoot%\System32\PimIndexMaintenance.dll,,,
Fri Jul 10 11:05:05 2015Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,
Fri Jul 10 11:05:05 2015Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Fri Jul 10 11:05:05 2015Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,;
Fri Jul 10 11:05:05 2015Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PortProxy,,,;
Fri Jul 10 11:05:05 2015Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,;
Fri Jul 10 11:05:05 2015Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,
```

Page 154

SYSTEM OUTPUT.txt
Fri Jul 10 11:05:05 2015Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,
Fri Jul 10 11:05:05 2015Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,Kernel driver,Manual,
Fri Jul 10 11:05:05 2015Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Fri Jul 10 11:05:05 2015Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,,
Fri Jul 10 11:05:05
2015Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Fri Jul 10 11:05:05
2015Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,RetailDemo\Parameters,,%SystemRoot%\system32\RDXService.dll,,,
Fri Jul 10 11:05:05
2015Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Fri Jul 10 11:05:05 2015Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Fri Jul 10 11:05:05 2015Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,
Fri Jul 10 11:05:05
2015Z,ScDeviceEnum\Parameters,,%SystemRoot%\System32\ScDeviceEnum.dll,,,
Fri Jul 10 11:05:05 2015Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Fri Jul 10 11:05:05 2015Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,
Fri Jul 10 11:05:05 2015Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,
Fri Jul 10 11:05:05 2015Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,
Fri Jul 10 11:05:05
2015Z,SensorService\Parameters,,%SystemRoot%\system32\SensorService.dll,,,
Fri Jul 10 11:05:05
2015Z,SessionEnv\Parameters,,%SystemRoot%\System32\sessenv.dll,,,
Fri Jul 10 11:05:05
2015Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,
Fri Jul 10 11:05:05
2015Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Fri Jul 10 11:05:05 2015Z,smphost\Parameters,,%Systemroot%\System32\smphost.dll,,,
Fri Jul 10 11:05:05
2015Z,SmsRouter\Parameters,,%SystemRoot%\system32\SmsRouterSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,
Fri Jul 10 11:05:05 2015Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,StateRepository\Parameters,,%SystemRoot%\system32\windows.staterepository.dll,
,,
Fri Jul 10 11:05:05 2015Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Fri Jul 10 11:05:05 2015Z,svsvc\Parameters,,%SystemRoot%\System32\svsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Fri Jul 10 11:05:05 2015Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Fri Jul 10 11:05:05
2015Z,SystemEventsBroker\Parameters,,%SystemRoot%\System32\SystemEventsBrokerServer.
dll,,,
Fri Jul 10 11:05:05
2015Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Fri Jul 10 11:05:05
2015Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Fri Jul 10 11:05:05
2015Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Fri Jul 10 11:05:05
2015Z,tiledatamodelsvc\Parameters,,%SystemRoot%\system32\tileobjserver.dll,,,
Fri Jul 10 11:05:05
2015Z,TimeBroker\Parameters,,%SystemRoot%\System32\TimeBrokerServer.dll,,,
Fri Jul 10 11:05:05 2015Z,Trkwks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Fri Jul 10 11:05:05 2015Z,TSDDD,,,,,
Fri Jul 10 11:05:05 2015Z,UGatherer,,,,,
Fri Jul 10 11:05:05 2015Z,UGTHRSVC,,,,,
Fri Jul 10 11:05:05
2015Z,UnistoreSvc\Parameters,,%SystemRoot%\System32\unistore.dll,,,
Page 155

SYSTEM OUTPUT.txt
```
Fri Jul 10 11:05:05 2015Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Fri Jul 10 11:05:05
2015Z,UserDataSvc\Parameters,,%SystemRoot%\System32\userdataservice.dll,,,
Fri Jul 10 11:05:05
2015Z,UserManager\Parameters,,%SystemRoot%\System32\usermgr.dll,,,
Fri Jul 10 11:05:05 2015Z,UsoSvc\Parameters,,%systemroot%\system32\usocore.dll,,,
Fri Jul 10 11:05:05
2015Z,VerifierExt,@%SystemRoot%\system32\drivers\VerifierExt.sys;-1000,system32\driv
ers\VerifierExt.sys,Kernel driver,Manual,
Fri Jul 10 11:05:05
2015Z,vmicguestinterface\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmicheartbeat\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmickvpexchange\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,vmicrdv\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmicshutdown\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmictimesync\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmicvmsession\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,vmicvss\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,w32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Fri Jul 10 11:05:05
2015Z,walletService\Parameters,,%SystemRoot%\system32\walletService.dll,,,
Fri Jul 10 11:05:05 2015Z,wbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,
Fri Jul 10 11:05:05 2015Z,wcmsvc\Parameters,,%SystemRoot%\System32\wcmsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Fri Jul 10 11:05:05
2015Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Fri Jul 10 11:05:05 2015Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Fri Jul 10 11:05:05 2015Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,
Fri Jul 10 11:05:05 2015Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WEPHOSTSVC\Parameters,,%systemroot%\system32\wephostsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Fri Jul 10 11:05:05 2015Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WiaRpc\Parameters,,%SystemRoot%\System32\wiarpc.dll,,,
Fri Jul 10 11:05:05
2015Z,WinHttpAutoProxySvc\Parameters,,%SystemRoot%\system32\winhttp.dll,,,
Fri Jul 10 11:05:05 2015Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WinSock2,,,,,
Fri Jul 10 11:05:05 2015Z,wlidsvc\Parameters,,%SystemRoot%\system32\wlidsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WmiApRpl,,,,,
Fri Jul 10 11:05:05 2015Z,workerdd,,,,,
Fri Jul 10 11:05:05
2015Z,workfolderssvc\Parameters,,%systemroot%\system32\workfolderssvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Fri Jul 10 11:05:05
2015Z,WpnService\Parameters,,%SystemRoot%\system32\WpnService.dll,,,
Fri Jul 10 11:05:05 2015Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WSearchIdxPi,,,,,
Fri Jul 10 11:05:05
2015Z,WSService\Parameters,,%SystemRoot%\System32\WSService.dll,,,
Fri Jul 10 11:05:05 2015Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Fri Jul 10 11:05:05 2015Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,
Fri Jul 10 11:05:05
```

Page 156

SYSTEM OUTPUT.txt
2015Z,XblAuthManager\Parameters,,%SystemRoot%\System32\XblAuthManager.dll,,,
Fri Jul 10 11:05:05
2015Z,XblGameSave\Parameters,,%SystemRoot%\System32\XblGameSave.dll,,,
Fri Jul 10 11:05:05
2015Z,XboxNetApiSvc\Parameters,,%SystemRoot%\system32\XboxNetApiSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,xmlprov,,,,,
Fri Jul 10 11:04:15
2015Z,TsUsbGD,@tsgenericusbdriver.inf;%TsUsbGD.DeviceDesc.Generic%;Remote Desktop
Generic USB Device,\SystemRoot\System32\drivers\TsUsbGD.sys,Kernel driver,Manual,
Fri Jul 10 11:04:15
2015Z,UrsChipidea,@urschipidea.inf;%UrsChipidea.ServiceName%;Chipidea USB
Role-Switch Driver,\SystemRoot\System32\drivers\urschipidea.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:15
2015Z,UrsSynopsys,@urssynopsys.inf;%UrsSynopsys.ServiceName%;Synopsys USB
Role-Switch Driver,\SystemRoot\System32\drivers\urssynopsys.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:13 2015Z,vhdmp,,\SystemRoot\System32\drivers\vhdmp.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:12 2015Z,AmdK8,@cpu.inf;%AmdK8.SvcDesc%;AMD K8 Processor
Driver,\SystemRoot\System32\drivers\amdk8.sys,Kernel driver,Manual,
Fri Jul 10 11:04:12 2015Z,AmdPPM,@cpu.inf;%AmdPPM.SvcDesc%;AMD Processor
Driver,\SystemRoot\System32\drivers\amdppm.sys,Kernel driver,Manual,
Fri Jul 10 11:04:12 2015Z,Processor,@cpu.inf;%Processor.SvcDesc%;Processor
Driver,\SystemRoot\System32\drivers\processr.sys,Kernel driver,Manual,
Fri Jul 10 11:04:11 2015Z,UfxChipidea,@ufxchipidea.inf;%UfxChipidea.ServiceName%;USB
Chipidea Controller,\SystemRoot\System32\drivers\UfxChipidea.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:11 2015Z,ufxsynopsys,@ufxsynopsys.inf;%ufxsynopsys.ServiceName%;USB
Synopsys Controller,\SystemRoot\System32\drivers\ufxsynopsys.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:08 2015Z,ibbus,@mlx4_bus.inf;%Ibbus.ServiceDesc%;Mellanox
InfiniBand Bus/AL (Filter Driver),\SystemRoot\System32\drivers\ibbus.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:08 2015Z,mlx4_bus,@mlx4_bus.inf;%MLX4BUS.ServiceDesc%;Mellanox
ConnectX Bus Enumerator,\SystemRoot\System32\drivers\mlx4_bus.sys,Kernel
driver,Manual,
Fri Jul 10 11:04:08 2015Z,ndfltr,@mlx4_bus.inf;%ndfltr.ServiceDesc%;NetworkDirect
Service,\SystemRoot\System32\drivers\ndfltr.sys,Kernel driver,Manual,
Fri Jul 10 11:04:08 2015Z,sermouse,@msmouse.inf;%sermouse.SvcDesc%;Serial Mouse
Driver,\SystemRoot\System32\drivers\sermouse.sys,Kernel driver,Manual,
Fri Jul 10 11:04:08 2015Z,WinMad,@mlx4_bus.inf;%WinMad.ServiceDesc%;WinMad
Service,\SystemRoot\System32\drivers\winmad.sys,Kernel driver,Manual,
Fri Jul 10 11:04:08 2015Z,WinVerbs,@mlx4_bus.inf;%WinVerbs.ServiceDesc%;WinVerbs
Service,\SystemRoot\System32\drivers\winverbs.sys,Kernel driver,Manual,
Fri Jul 10 11:04:04 2015Z,hidinterrupt,@hidinterrupt.inf;%HID.SvcDesc%;Common Driver
for HID Buttons implemented with
interrupts,\SystemRoot\System32\drivers\hidinterrupt.sys,Kernel driver,Manual,
Fri Jul 10 11:04:04 2015Z,WacomPen,@hiddigi.inf;%WacomPen.SVCDESC%;Wacom Serial Pen
HID Driver,\SystemRoot\System32\drivers\wacompen.sys,Kernel driver,Manual,
Fri Jul 10 11:04:03 2015Z,acpitime,@acpitime.inf;%AcpiTime.SvcDesc%;ACPI Wake Alarm
Driver,\SystemRoot\System32\drivers\acpitime.sys,Kernel driver,Manual,
Fri Jul 10 11:04:03 2015Z,bcmfn2,@bcmfn2.inf;%bcmfn2.SVCDESC%;bcmfn2
Service,\SystemRoot\System32\drivers\bcmfn2.sys,Kernel driver,Manual,
Fri Jul 10 11:04:03 2015Z,ErrDev,@errdev.inf;%ERRDEV.SvcDesc%;Microsoft Hardware
Error Device Driver,\SystemRoot\System32\drivers\errdev.sys,Kernel driver,Manual,
Fri Jul 10 11:04:03
2015Z,genericusbfn,@genericusbfn.inf;%genericusbfn.ServiceName%;Generic USB Function
Class,\SystemRoot\System32\drivers\genericusbfn.sys,Kernel driver,Manual,
Fri Jul 10 11:04:01 2015Z,wfpcapture,@wfpcapture.inf;%WfpCapture_Desc%;Microsoft WFP
Message Capture,\SystemRoot\System32\drivers\wfpcapture.sys,Kernel driver,Manual,
Fri Jul 10 11:04:01 2015Z,xinputhid,@xinputhid.inf;%xinputhid.SvcDesc%;XINPUT HID
Filter Driver,\SystemRoot\System32\drivers\xinputhid.sys,Kernel driver,Manual,
Page 157

SYSTEM OUTPUT.txt
Fri Jul 10 11:04:00 2015Z,usbcir,@usbcir.inf;%usbcir.SVCDESC%;eHome Infrared
Receiver (USBCIR),\SystemRoot\System32\drivers\usbcir.sys,Kernel driver,Manual,
Fri Jul 10 11:03:59 2015Z,circlass,@circlass.inf;%circlass.SVCDESC%;Consumer IR
Devices,\SystemRoot\System32\drivers\circlass.sys,Kernel driver,Manual,
Fri Jul 10 11:03:59 2015Z,HidBth,@hidbth.inf;%HIDBTH.SvcDesc%;Microsoft Bluetooth
HID Miniport,\SystemRoot\System32\drivers\hidbth.sys,Kernel driver,Manual,
Fri Jul 10 11:03:59 2015Z,HidIr,@hidir.inf;%HIDIR.SvcDesc%;Microsoft Infrared HID
Driver,\SystemRoot\System32\drivers\hidir.sys,Kernel driver,Manual,
Fri Jul 10 11:03:58 2015Z,fcvsc,,\SystemRoot\System32\drivers\fcvsc.sys,Kernel
driver,Manual,
Fri Jul 10 11:03:58 2015Z,vpci,@wvpci.inf;%vpci.SVCDESC%;Microsoft Hyper-V Virtual
PCI Bus,\SystemRoot\System32\drivers\vpci.sys,Kernel driver,Manual,
------------------------------------
svc_plus v.20120625
(System) Lists services/drivers in Services key by LastWrite times in a short format
with warnings for type mismatches
^^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.

ControlSet001\Services
Lists services/drivers in Services key by LastWrite times in a short format with
warnings for type mismatches
^^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.

Thu Apr 21 04:41:25 2016Z,mfeavfk,McAfee Inc.
mfeavfk,system32\drivers\mfeavfk.sys,,Manual,
Thu Apr 21 04:41:19 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common
Files\McAfee\SystemCore\\mfemms.exe",,Auto Start,****LocalSystem
Thu Apr 21 04:41:16 2016Z,mfeaack,McAfee Inc.
mfeaack,system32\drivers\mfeaack.sys,,Manual,
Thu Apr 21 04:41:15 2016Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor
Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",,Auto
Start,****LocalSystem
Thu Apr 21 04:41:15 2016Z,McAPExe,McAfee AP Service,"C:\Program
Files\McAfee\MSC\McAPExe.exe",,Auto Start,****LocalSystem
Thu Apr 21 04:41:15 2016Z,McMPFSvc,McAfee Personal Firewall Service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,,Auto
Start,****LocalSystem
Thu Apr 21 04:41:15 2016Z,McProxy,McAfee Proxy Service,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,,Auto Start,****LocalSystem
Thu Apr 21 04:41:15
2016Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,
Thu Apr 21 03:24:59
2016Z,MBAMSwissArmy,MBAMSwissArmy,\??\C:\Windows\system32\drivers\MBAMSwissArmy.sys,
,Manual,
Thu Apr 21 03:20:08 2016Z,mfefirek,McAfee Inc.
mfefirek,system32\drivers\mfefirek.sys,,Manual,
Thu Apr 21 03:19:52 2016Z,cfwids,McAfee Inc.
cfwids,system32\drivers\cfwids.sys,,Manual,
Thu Apr 21 03:19:50 2016Z,mfencbdc,McAfee Inc.
mfencbdc,\SystemRoot\system32\DRIVERS\mfencbdc.sys,,Manual,
Thu Apr 21 03:19:31 2016Z,UmPass,@umpass.inf;%UmPass.SVCDESC%;Microsoft UMPass
Driver,\SystemRoot\System32\drivers\umpass.sys,,Manual,
Thu Apr 21 03:19:16 2016Z,tunnel,@nettun.inf;%TUNNEL.Service.DisplayName%;Microsoft
Tunnel Miniport Adapter Driver,\SystemRoot\System32\drivers\tunnel.sys,,Manual,
Thu Apr 21 03:19:15
Page 158

SYSTEM OUTPUT.txt
2016Z,vwifimp,@%SystemRoot%\System32\drivers\vwifimp.sys;-261,\SystemRoot\System32\d
rivers\vwifimp.sys,,Manual,
Thu Apr 21 03:19:03
2016Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,
Thu Apr 21 03:18:58
2016Z,BasicDisplay,,\SystemRoot\System32\drivers\BasicDisplay.sys,,System Start,
Thu Apr 21 03:18:58 2016Z,monitor,@monitor.inf;%Monitor.SVCDESC%;Microsoft Monitor
Class Function Driver Service,\SystemRoot\System32\drivers\monitor.sys,,Manual,
Thu Apr 21 03:18:57
2016Z,BtFilter,BtFilter,\SystemRoot\system32\DRIVERS\btfilter.sys,,Manual,
Thu Apr 21 03:18:57 2016Z,BTHUSB,@bth.inf;%BTHUSB.SvcDesc%;Bluetooth Radio USB
Driver,\SystemRoot\System32\Drivers\BTHUSB.sys,,Manual,
Thu Apr 21 03:18:57 2016Z,RTSUER,@oem14.inf;%RtsUER%;Realtek USB Card Reader -
UER,\SystemRoot\system32\Drivers\RtsUer.sys,,Manual,
Thu Apr 21 03:18:56 2016Z,HidUsb,@input.inf;%HID.SvcDesc%;Microsoft HID Class
Driver,\SystemRoot\System32\drivers\hidusb.sys,,Manual,
Thu Apr 21 03:18:56 2016Z,usbccgp,@usb.inf;%GenericParent.SvcDesc%;Microsoft USB
Generic Parent Driver,\SystemRoot\System32\drivers\usbccgp.sys,,Manual,
Thu Apr 21 03:18:56 2016Z,usbvideo,@usbvideo.inf;%USBVideo.SvcDesc%;USB Video Device
(WDM),\SystemRoot\System32\Drivers\usbvideo.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,ETDI2C,@oem13.inf;%ELANI2CDeviceDesc%;ELAN I2C Filter
Driver,\SystemRoot\system32\DRIVERS\ETDI2C.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,hidi2c,@hidi2c.inf;%hidi2c.SVCDESC%;Microsoft I2C HID
Miniport Driver,\SystemRoot\System32\drivers\hidi2c.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,IntcDAud,@oem6.inf;%IntcDAud.SvcDesc%;Intel(R) Display
Audio,\SystemRoot\system32\DRIVERS\IntcDAud.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,mouclass,@msmouse.inf;%mouclass.SvcDesc%;Mouse Class
Driver,\SystemRoot\System32\drivers\mouclass.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,mouhid,@msmouse.inf;%MOUHID.SvcDesc%;Mouse HID
Driver,\SystemRoot\System32\drivers\mouhid.sys,,Manual,
Thu Apr 21 03:18:55
2016Z,mshidkmdf,,\SystemRoot\System32\drivers\mshidkmdf.sys,,Manual,
Thu Apr 21 03:18:55 2016Z,MTConfig,@mtconfig.inf;%MTConfig.SVCDESC%;Microsoft Input
Configuration Driver,\SystemRoot\System32\drivers\MTConfig.sys,,Manual,
Thu Apr 21 03:18:54 2016Z,IntcAzAudAddService,Service for Realtek HD Audio
(WDM),\SystemRoot\system32\drivers\RTKVHD64.sys,,Manual,
Thu Apr 21 03:18:54 2016Z,ksthunk,Kernel Streaming
Thunks,\SystemRoot\system32\drivers\ksthunk.sys,,Manual,
Thu Apr 21 03:18:54 2016Z,USBHUB3,@usbhub3.inf;%UsbHub3.SVCDESC%;SuperSpeed
Hub,\SystemRoot\System32\drivers\UsbHub3.sys,,Manual,
Thu Apr 21 03:18:51 2016Z,mssmbios,@mssmbios.inf;%mssmbios_svcdesc%;Microsoft System
Management BIOS Driver,\SystemRoot\System32\drivers\mssmbios.sys,,System Start,
Thu Apr 21 03:18:49 2016Z,ACPI,@acpi.inf;%ACPI.SvcDesc%;Microsoft ACPI
Driver,System32\drivers\ACPI.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,athr,@oem10.inf;%ATHR.Service.DispName%;Qualcomm Atheros
Extensible Wireless LAN device
driver,\SystemRoot\System32\drivers\athw10x.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,cdrom,@cdrom.inf;%cdrom_ServiceDesc%;CD-ROM
Driver,\SystemRoot\System32\drivers\cdrom.sys,,System Start,
Thu Apr 21 03:18:49 2016Z,CmBatt,@cmbatt.inf;%CmBatt.SvcDesc%;Microsoft ACPI Control
Method Battery Driver,\SystemRoot\System32\drivers\CmBatt.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,disk,@disk.inf;%disk_ServiceDesc%;Disk
Driver,System32\drivers\disk.sys,,Boot Start,
Thu Apr 21 03:18:49
2016Z,EhStorClass,@%SystemRoot%\system32\drivers\EhStorClass.sys;-100,System32\drive
rs\EhStorClass.sys,,Boot Start,
Thu Apr 21 03:18:49
2016Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.
sys,,Boot Start,
Thu Apr 21 03:18:49,2016Z,GPIO,@oem4.inf;%GPIO.SVCDESC%;Intel SoC GPIO Controller
Driver,\SystemRoot\System32\drivers\iaiogpioe.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,HDAudBus,@hdaudbus.inf;%HDAudBus.SVCDESC%;Microsoft UAA
Bus Driver for High Definition
Page 159

SYSTEM OUTPUT.txt
Audio,\SystemRoot\System32\drivers\HDAudBus.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,i8042prt,@keyboard.inf;%i8042prt.SvcDesc%;i8042 Keyboard
and PS/2 Mouse Port Driver,\SystemRoot\System32\drivers\i8042prt.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,iaioi2c,@oem5.inf;%Driver_Service.Desc%;I2C Controller
Service,\SystemRoot\System32\drivers\iaioi2ce.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,igfx,,\SystemRoot\system32\DRIVERS\igdkmd64.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,intelpep,@intelpep.inf;%INTELPEP.SVCDESC%;Intel(R) Power
Engine Plug-in Driver,System32\drivers\intelpep.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,intelppm,@cpu.inf;%IntelPPM.SvcDesc%;Intel Processor
Driver,\SystemRoot\System32\drivers\intelppm.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,kbdclass,@keyboard.inf;%kbdclass.SvcDesc%;Keyboard Class
Driver,\SystemRoot\System32\drivers\kbdclass.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,mfewfpk,McAfee Inc.
mfewfpk,system32\drivers\mfewfpk.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,msisadrv,,System32\drivers\msisadrv.sys,,Boot Start,
Thu Apr 21 03:18:49
2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partm
gr.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,pci,@pci.inf;%pci_svcdesc%;PCI Bus
Driver,System32\drivers\pci.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,,Boot
Start,
Thu Apr 21 03:18:49 2016Z,rt640x64,@oem12.inf;%rt640.Service.DispName%;Realtek RT640
NT Driver,\SystemRoot\System32\drivers\rt640x64.sys,,Manual,
Thu Apr 21 03:18:49
2016Z,storahci,@mshdc.inf;%storahci_ServiceDescription%;Microsoft Standard SATA AHCI
Driver,System32\drivers\storahci.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,TXEIx64,@oem2.inf;%TEE_SvcDesc%;Intel(R) Trusted Execution
Engine Interface ,\SystemRoot\System32\drivers\TXEIx64.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,UEFI,@uefi.inf;%UEFI.SvcDesc%;Microsoft UEFI
Driver,\SystemRoot\System32\drivers\UEFI.sys,,Manual,
Thu Apr 21 03:18:49 2016Z,USBXHCI,@usbxhci.inf;%PCI\CC_0C0330.DeviceDesc%;USB xHCI
Compliant Host Controller,\SystemRoot\System32\drivers\USBXHCI.SYS,,Manual,
Thu Apr 21 03:18:49 2016Z,volsnap,@volume.inf;%VolumeClassName%;Storage
volumes,System32\drivers\volsnap.sys,,Boot Start,
Thu Apr 21 03:18:49
2016Z,vwifibus,@%SystemRoot%\System32\drivers\vwifibus.sys;-257,\SystemRoot\System32
\drivers\vwifibus.sys,,Manual,
Thu Apr 21 03:18:49
2016Z,wdf01000,@%SystemRoot%\system32\drivers\wdf01000.sys;-1000,system32\drivers\Wd
f01000.sys,,Boot Start,
Thu Apr 21 03:18:49 2016Z,WmiAcpi,@wmiacpi.inf;%WMIMAP.SvcDesc%;Microsoft Windows
Management Interface for ACPI,\SystemRoot\System32\drivers\wmiacpi.sys,,Manual,
Thu Apr 21 03:18:48
2016Z,BasicRender,,\SystemRoot\System32\drivers\BasicRender.sys,,System Start,
Thu Apr 21 03:18:48
2016Z,CompositeBus,@compositebus.inf;%CompositeBus.SVCDESC%;Composite Bus Enumerator
Driver,\SystemRoot\System32\DriverStore\FileRepository\compositebus.inf_amd64_98334b
a6e76853ba\CompositeBus.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,iwdbus,@oem9.inf;%iwdbus.SVCDESC%;IWD Bus
Enumerator,\SystemRoot\System32\drivers\iwdbus.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,kdnic,@kdnic.inf;%KdNic.Service.DispName%;Microsoft Kernel
Debug Network Miniport (NDIS 6.20),\SystemRoot\System32\drivers\kdnic.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,LMDriver,@oem16.inf;%LMDriver.SVCDESC%;Launch Manager
Wireless Driver,\SystemRoot\System32\drivers\LMDriver.sys,,Manual,
Thu Apr 21 03:18:48
2016Z,NdisVirtualBus,@%SystemRoot%\System32\drivers\NdisVirtualBus.sys;-200,\SystemR
oot\System32\drivers\NdisVirtualBus.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,RadioShim,@oem16.inf;%RadioShim.SVCDESC%;Shim for HID-KMDF
Interface layer,\SystemRoot\System32\drivers\RadioShim.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,rdpbus,@rdpbus.inf;%rdpbus_svcdesc%;Remote Desktop Device
Redirector Bus Driver,\SystemRoot\System32\drivers\rdpbus.sys,,Manual,
Thu Apr 21 03:18:48 2016Z,spaceport,@spaceport.inf;%Spaceport_ServiceDesc%;Storage
Page 160

SYSTEM OUTPUT.txt

Spaces Driver,System32\drivers\spaceport.sys,,Boot Start,
Thu Apr 21 03:18:48 2016z,tap0901,@oem23.inf;%DeviceDescription%;TAP-Windows Adapter
V9,\SystemRoot\System32\drivers\tap0901.sys,,Manual,
Driver,\SystemRoot\System32\drivers\tap0901.sys,,Manual,
Thu Apr 21 03:18:48 2016z,umbus,@umbus.inf;%umbus.SVCDESC%;UMBus Enumerator
Driver,\SystemRoot\System32\drivers\umbus.sys,,Manual,
Thu Apr 21 03:18:48 2016z,vdrvroot,@vdrvroot.inf;%vdrvroot_svcdesc%;Microsoft
Virtual Drive Enumerator,\SystemRoot\System32\drivers\vdrvroot.sys,,Boot Start,
Driver,System32\drivers\volmgr.sys,,Boot Start,
Thu Apr 21 03:18:48 2016z,volmgr,@volmgr.inf;%volmgr_svcdesc%;Volume Manager
Driver,\SystemRoot\system32\drivers\volmgr.sys,,Boot Start,
Thu Apr 21 03:15:49 2016z,mfesapsn,McAfee Process Start Notification
Service,\??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,,Manual,
Thu Apr 21 03:15:18 2016z,McPvDrv,McPvDrv
Driver,\SystemRoot\system32\drivers\McPvDrv.sys,,<<<Auto Start,
Thu Apr 21 03:15:06 2016z,MSK80Service,McAfee Anti-Spam Service,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvcHost.exe" /McCoreSvc,,Auto
Start,****LocalSystem
Thu Apr 21 03:14:14 2016z,Hipshieldk,McAfee Inc.
Hipshieldk,system32\drivers\Hipshieldk.sys,,Manual,
Thu Apr 21 03:13:53 2016z,WdBoot,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-390,\SystemRoot\system32\drivers\wdBoot.sys,,Manual,
Thu Apr 21 03:13:53 2016z,WdFilter,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-330,\SystemRoot\system32\drivers\wdFilter.sys,,Manual,
Thu Apr 21 03:13:47 2016z,mfehidk,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,,Boot Start,
Thu Apr 21 03:13:47 2016z,WinDefend,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-310,,"%ProgramFiles%\Windows
Defender\MsMpEng.exe",,Manual,
Thu Apr 21 03:13:46 2016z,WdNisDrv,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-370,\SystemRoot\system32\drivers\WdNisDrv.sys,,Manual,
Thu Apr 21 03:13:35 2016z,McODS,McAfee Scanner,"C:\Program
Files\McAfee\VirusScan\mcods.exe",,Manual,****LocalSystem
Thu Apr 21 03:13:25 2016z,McNaiAnn,McAfee VirusScan Announcer,"C:\Program
Files\Common Files\McAfee\Platform\McSvcHost\McSvcHost.exe"/McCoreSvc,,Auto
Start,****LocalSystem
Thu Apr 21 03:12:49 2016z,mfencrk,McAfee Inc.
mfencrk,\SystemRoot\system32\DRIVERS\mfencrk.sys,,Manual,
Thu Apr 21 03:12:03 2016z,McBootDelayStartSvc,McAfee Boot Delay Start
Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvcHost.exe"
/McCoreSvc,,Auto Start,****LocalSystem
Thu Apr 21 03:12:02 2016z,mcpltsvc,McAfee Platform Services,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvcHost.exe" /McCoreSvc,,Auto Start,****LocalSystem
Thu Apr 21 03:11:46 2016z,PEFService,Intel Security PEF Service,"C:\Program
Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",,Auto
Start,****LocalSystem
Thu Apr 21 03:11:37 2016z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common
Files\McAfee\CSP\1.9.656.0\McCSPServiceHost.exe",,Auto Start,****LocalSystem
Thu Apr 21 03:10:59 2016z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common
Files\McAfee\Platform\McSvcHost\McSvcHost.exe" /McCoreSvc,,Auto Start,****LocalSystem
Thu Apr 21 03:10:58 2016z,mfefire,McAfee Firewall Core Service,"C:\Program
Files\Common Files\McAfee\SystemCore\\mfefire.exe",,Manual,****LocalSystem
Thu Apr 21 03:10:57 2016z,mfevtp,McAfee Validation Trust Protection
Service,"C:\Windows\system32\mfevtps.exe",,Manual,****LocalSystem
Thu Apr 21 03:10:48 2016z,mfeelamk,mfeelamk,McAfee Inc.
mfeelamk,system32\drivers\mfeelamk.sys,,Boot Start,
Thu Apr 21 03:08:54 2016z,ModuleCoreService,McAfee Module Core Service,"C:\Program
Files\Common Files\McAfee\ModuleCore\ModuleCoreService.exe",,Auto
Start,****LocalSystem
Thu Apr 21 03:00:51
2016z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Auto Start,****LocalSystem

Page 161

SYSTEM OUTPUT.txt

Sun Apr 17 00:48:02 2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\TrustedInstaller.exe,,Manual,****localSystem
Sun Apr 17 00:47:20 2016Z,DeviceInstall\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Sun Apr 17 00:44:02 2016Z,BthLEEnum,@bthleenum.inf;%BthLEEnum.SVCDESC%;Bluetooth Low Energy Driver,\SystemRoot\System32\drivers\BthLEEnum.sys,,Manual,
Sun Apr 17 00:44:02 2016Z,Parport,@msports.inf;%Parport.SVCDESC%;Parallel port driver,\SystemRoot\System32\drivers\parport.sys,,Manual,
Sun Apr 17 00:44:02 2016Z,Serenum,@msports.inf;%Serenum.SVCDESC%;Serenum Filter Driver,\SystemRoot\System32\drivers\serenum.sys,,Manual,
Sun Apr 17 00:44:02 2016Z,Serial,@msports.inf;%Serial.SVCDESC%;Serial port driver,\SystemRoot\System32\drivers\serial.sys,,Manual,
Sun Apr 17 00:44:02 2016Z,usbser,@usbser.inf;%UsbSerial.DriverDesc%;Microsoft USB Serial Driver,\SystemRoot\System32\drivers\usbser.sys,,Manual,
Sun Apr 17 00:44:02 2016Z,USBSTOR,@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass Storage Driver,\SystemRoot\System32\drivers\USBSTOR.SYS,,Manual,
Tue Apr 12 20:56:49 2016Z,YahooAUService,Yahoo! Updater,"C:\Program Files (x86)\Yahoo!\SoftwareUpdate\YahooAUService.exe",,Auto Start,****LocalSystem
Tue Apr  5 22:21:01 2016Z,MSPCLOCK,@ksfilter.inf;%MSPCLOCK.DeviceDesc%;Microsoft Streaming Clock Proxy,\SystemRoot\system32\drivers\MSPCLOCK.sys,,Manual,
Tue Apr  5 22:21:00 2016Z,MSPQM,@ksfilter.inf;%MSPQM.DeviceDesc%;Microsoft Streaming Quality Manager Proxy,\SystemRoot\system32\drivers\MSPQM.sys,,Manual,
Sat Apr  2 16:10:08 2016Z,BthAvrcpTg,@bthaudhid.inf;%BthAvrcpTg_SvcDesc%;Bluetooth Audio/Video Remote Control HID,\SystemRoot\System32\drivers\BthAvrcpTg.sys,,Manual,
Sat Apr  2 16:08:56 2016Z,BthPan,@bthpan.inf;%BthPan.DisplayName%;Bluetooth Device (Personal Area Network),\SystemRoot\System32\drivers\bthpan.sys,,Manual,
Sat Apr  2 16:08:55 2016Z,BthEnum,@bth.inf;%BthEnum.SVCDESC%;Bluetooth Enumerator Service,\SystemRoot\System32\drivers\BthEnum.sys,,Manual,
Sat Apr  2 16:08:55 2016Z,RFCOMM,@tdibth.inf;%RFCOMM.DisplayName%;Bluetooth Device (RFCOMM Protocol TDI),\SystemRoot\System32\drivers\rfcomm.sys,,Manual,
Tue Mar 29 09:31:18 2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,System32\DRIVERS\ndistapi.sys,,Manual,
Tue Mar 29 09:31:18 2016Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,\SystemRoot\System32\drivers\ndiswan.sys,,Manual,
Tue Mar 29 09:31:18 2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,\SystemRoot\System32\drivers\raspptp.sys,,Manual,
Tue Mar 29 09:31:18 2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,\SystemRoot\System32\drivers\rasl2tp.sys,,Manual,
Tue Mar 29 09:31:18 2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,\SystemRoot\System32\drivers\raspppoe.sys,,Manual,
Tue Mar 29 09:31:17 2016Z,RasAgileVpn,@netavpna.inf;%Svc-Mp-AgileVpn-DispName%;WAN Miniport (IKEv2),\SystemRoot\System32\drivers\AgileVpn.sys,,Manual,
Tue Mar 29 09:31:16 2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,\SystemRoot\System32\drivers\rassstp.sys,,Manual,
Tue Mar 29 09:29:40 2016Z,DeviceAssociationService,@%SystemRoot%\system32\das.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Mar 29 09:22:07 2016Z,lltdio,@%SystemRoot%\system32\lltdres.dll;-6,system32\drivers\lltdio.sys,,<<<< Auto Start,
Tue Mar 29 09:22:07 2016Z,ndiswanlegacy,@%systemroot%\system32\rascfg.dll;-32014,System32\DRIVERS\ndiswan.sys,,Manual,
Tue Mar 29 09:22:07 2016Z,rspndr,@%SystemRoot%\system32\lltdres.dll;-5,system32\drivers\rspndr.sys,,<<<< Auto Start,

Page 162

SYSTEM OUTPUT.txt

Tue Mar 29 09:22:07
2016Z,wanarp,@%systemroot%\system32\rascfg.dll;-32011,System32\DRIVERS\wanarp.sys,,<
<<<Auto Start,
Tue Mar 29 09:22:07
2016Z,wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,System32\DRIVERS\wanarp.sys,
,Manual,
Sun Mar 27 13:05:49 2016Z,ESProtectionDriver,Malwarebytes
Anti-Exploit,\??\C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae64.sys,,System
Start,
Sun Mar 27 13:05:49 2016Z,MbaeSvc,Malwarebytes Anti-Exploit Service,"C:\Program
Files (x86)\Malwarebytes Anti-Exploit\mbae-svc.exe",,Auto Start,****LocalSystem
Wed Mar 23 10:11:59 2016Z,OpenVPNService,OpenVPN Service,"C:\Program Files
(x86)\HMA! Pro VPN\bin\openvpnserv.exe",,Manual,****LocalSystem
Wed Mar 23 10:11:16 2016Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Wed Mar 23 10:11:15 2016Z,ndproxy,@%SystemRoot%\system32\drivers\todo.sys;-101;NDIS
Proxy,System32\DRIVERS\NDProxy.sys,,Manual,
Wed Mar 23 09:50:47 2016Z,BrSerIb,@oem20.inf;%BrSerIb.SvcDesc%;Brother Serial
Interface Driver(WDM),\SystemRoot\system32\DRIVERS\BrSerIb.sys,,Manual,
Wed Mar 23 09:50:47 2016Z,BrUsbSIb,@oem20.inf;%BrUsbSIb.SvcDesc%;Brother Serial USB
Driver(WDM),\SystemRoot\system32\DRIVERS\BrUsbSIb.sys,,Manual,
Wed Mar 23 09:50:47 2016Z,usbprint,@usbprint.inf;%USBPRINT.SvcDesc%;Microsoft USB
PRINTER Class,\SystemRoot\System32\drivers\usbprint.sys,,Manual,
Wed Mar 23 09:50:47 2016Z,usbscan,@sti.inf;%usbscan.SvcDesc%;USB Scanner
Driver,\SystemRoot\system32\DRIVERS\usbscan.sys,,Manual,
Wed Mar 23 09:50:26 2016Z,stornvme,@stornvme.inf;%StorNVMe_ServiceDesc%;Microsoft
Standard NVM Express Driver,System32\drivers\stornvme.sys,,Boot Start,
Wed Mar 23 09:48:50 2016Z,BthHFEnum,@bthhfenum.inf;%BthHFEnum.SVCDESC%;Bluetooth
Hands-Free Audio and Call Control HID
Enumerator,\SystemRoot\System32\drivers\bthhfenum.sys,,Manual,
Wed Mar 23 09:48:50
2016Z,BthHFSrv,@%SystemRoot%\System32\BthHFSrv.dll;-103,%SystemRoot%\System32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Wed Mar 23 09:48:50 2016Z,BthHFSrv\Parameters,,%SystemRoot%\System32\BthHFSrv.dll,,,
Wed Mar 23 09:48:50 2016Z,BTHPORT,@bth.inf;%BTHPORT.SvcDesc%;Bluetooth Port
Driver,\SystemRoot\System32\Drivers\BTHport.sys,,Manual,
Wed Mar 23 09:48:50
2016Z,buttonconverter,@buttonconverter.inf;%btnconv.SvcDesc%;Service for Portable
Device Control devices,\SystemRoot\System32\drivers\buttonconverter.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,drmkaud,@wdmaudio.inf;%drmkaud.SvcDesc%;Microsoft Trusted
Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,msgpiowin32,@msgpiowin32.inf;%GPIO.SvcDesc%;Common Driver
for Buttons; DockMode and Laptop/Slate
Indicator,\SystemRoot\System32\drivers\msgpiowin32.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,sdbus,,\SystemRoot\System32\drivers\sdbus.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,usbehci,@usbport.inf;%EHCIMP.SvcDesc%;Microsoft USB 2.0
Enhanced Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbehci.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,usbhub,@usbport.inf;%ROOTHUB.SvcDesc%;Microsoft USB
Standard Hub Driver,\SystemRoot\System32\drivers\usbhub.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,usbohci,@usbport.inf;%OHCIMP.SvcDesc%;Microsoft USB Open
Host Controller Miniport Driver,\SystemRoot\System32\drivers\usbohci.sys,,Manual,
Wed Mar 23 09:48:50 2016Z,usbuhci,@usbport.inf;%UHCIMP.SvcDesc%;Microsoft USB
Universal Host Controller Miniport
Driver,\SystemRoot\System32\drivers\usbuhci.sys,,Manual,
Wed Mar 23 09:41:44 2016Z,BrYNSvc,BrYNSvc,"C:\Program Files
(x86)\Browny02\BrYNSvc.exe",,Manual,****LocalSystem
Wed Mar 23 09:25:17
2016Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.ex
e -k imgsvc,,Auto Start,****NT Authority\LocalService
Tue Mar 22 13:52:39
2016Z,MsBridge,@%SystemRoot%\system32\bridgeres.dll;-1,System32\drivers\bridge.sys,,
Manual,
Tue Mar 22 13:52:38 2016Z,Ndisuio,NDIS Usermode I/O
Page 163

SYSTEM OUTPUT.txt

Protocol,system32\drivers\ndisuio.sys,,Manual,
Tue Mar 22 13:52:38 2016Z,xboxgip,@xboxgip.inf;%XBOXGIP_Desc%;Xbox Game Input
Protocol Driver,\SystemRoot\System32\drivers\xboxgip.sys,,Manual,
Tue Mar 22 13:31:01 2016Z,CCDMonitorService,CCDMonitorService,C:\Program Files
(x86)\Acer\AOP Framework\CCDMonitorService.exe,,Auto Start,****LocalSystem
Tue Mar 22 13:31:00 2016Z,ose,Office Source Engine,"C:\Program Files (x86)\Common
Files\Microsoft Shared\Source Engine\OSE.EXE",,Manual,****LocalSystem
Tue Mar 22 13:18:45
2016Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.ex
e -k netsvcs,,Auto Start,****LocalSystem
Tue Mar 22 13:16:27 2016Z,MSDTC Bridge 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,MSDTC Bridge 4.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,ServiceModelEndpoint 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,ServiceModelOperation 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,ServiceModelService 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,SMSvcHost 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,SMSvcHost 4.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,Windows Workflow Foundation 3.0.0.0,,,^^^^,,
Tue Mar 22 13:16:27 2016Z,Windows Workflow Foundation 4.0.0.0,,,^^^^,,
Tue Mar 22 13:15:54 2016Z,intaud_WaveExtensible,@oem8.inf;%INTAUD_WEX.SvcDesc%;Intel
WiDi Audio Device,\SystemRoot\system32\drivers\intelaud.sys,,Manual,
Tue Mar 22 13:15:48 2016Z,MSKSSRV,@ksfilter.inf;%MSKSSRV.DeviceDesc%;Microsoft
Streaming Service Proxy,\SystemRoot\system32\drivers\MSKSSRV.sys,,Manual,
Tue Mar 22 13:15:48 2016Z,MSTEE,@ksfilter.inf;%MSTEE.DeviceDesc%;Microsoft Streaming
Tee/Sink-to-Sink Converter,\SystemRoot\system32\drivers\MSTEE.sys,,Manual,
Tue Mar 22 13:15:31 2016Z,igfxCUIService1.0.0.0,Intel(R) HD Graphics Control Panel
Service,%SystemRoot%\system32\igfxCUIService.exe,,Auto Start,****LocalSystem
Tue Mar 22 13:06:05 2016Z,iphlpsvc\Parameters,,%SystemRoot%\System32\iphlpsvc.dll,,,
Tue Mar 22 12:21:54
2016Z,EventLog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost
.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Mar 22 12:20:09 2016Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,
Tue Mar 22 11:54:41 2016Z,MBAMScheduler,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamscheduler.exe",,Auto Start,****LocalSystem
Tue Mar 22 11:54:39 2016Z,MBAMService,,"C:\Program Files (x86)\Malwarebytes
Anti-Malware\mbamservice.exe",,Auto Start,****LocalSystem
Tue Mar 22 11:54:39
2016Z,MBAMWebAccessControl,,\??\C:\Windows\system32\drivers\mwac.sys,,Manual,
Tue Mar 22 11:54:38
2016Z,MBAMProtector,,\??\C:\Windows\system32\drivers\mbam.sys,,Manual,
Tue Mar 22 11:21:46 2016Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,,Manual,****LocalSystem
Tue Mar 22 10:37:21 2016Z,odserv,Microsoft Office Diagnostics Service,"C:\Program
Files (x86)\Common Files\Microsoft
Shared\OFFICE12\ODSERV.EXE",,Manual,****LocalSystem
Fri Sep 11 09:45:22
2015Z,WpdUpFltr,@%systemroot%\System32\drivers\WpdUpFltr.sys;-100,System32\drivers\W
pdUpFltr.sys,,Manual,
Fri Sep 11 09:45:22
2015Z,WUDFWpdFs,,\SystemRoot\system32\DRIVERS\WUDFRd.sys,,Manual,++++\Driver\WudfRd
Thu Aug 13 23:24:15
2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\Se
archIndexer.exe /Embedding,,Auto Start,****LocalSystem
Thu Aug 13 23:03:20
2015Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,,Manual,****NT
AUTHORITY\NetworkService
Thu Aug 13 22:52:11 2015Z,UcmUcsi,@ucmucsi.inf;%UcmUcsi.ServiceName%;USB Connector
Manager UCSI Client,\SystemRoot\System32\drivers\UcmUcsi.sys,,Manual,
Thu Aug 13 22:37:27 2015Z,ePowerSvc,ePower Service,"C:\Program Files\Acer\Acer Power
Management\ePowerSvc.exe",,Manual,****LocalSystem
Thu Aug 13 22:35:41 2015Z,QALSvc,Quick Access Local Service,"C:\Program
Files\Acer\Acer Quick Access\QALSvc.exe",,Manual,****NT AUTHORITY\LocalService
Thu Aug 13 22:35:41 2015Z,QASvc,Quick Access Service,"C:\Program Files\Acer\Acer
Page 164

SYSTEM OUTPUT.txt
Quick Access\QASvc.exe",,Manual,****LocalSystem
Thu Aug 13 22:34:01 2015Z,Dashlane Upgrade Service,,"C:\Program Files
(x86)\Dashlane\Upgrade\DashlaneUpgradeService.exe",,Auto Start,****LocalSystem
Thu Aug 13 22:33:48 2015Z,Amazon 1Button App Service,Amazon 1Button App
Service,"c:\Program Files
(x86)\Amazon\Amazon1ButtonApp\Amazon1ButtonService64.Exe",,Auto
Start,****LocalSystem
Thu Aug 13 22:25:21 2015Z,AtherosSvc,AtherosSvc,"C:\Program Files (x86)\Qualcomm
Atheros\Bluetooth Suite\adminservice.exe",,Auto Start,****LocalSystem
Thu Aug 13 22:21:05 2015Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,
Thu Aug 13 22:19:13 2015Z,ICCS,Intel(R) Integrated Clock Controller Service -
Intel(R) ICCS,"C:\Program Files (x86)\Intel\Intel(R) Integrated Clock Controller
Service\ICCProxy.exe",,Manual,****LocalSystem
Thu Aug 13 22:19:11 2015Z,ialm,,,^^^^,,
Thu Aug 13 22:15:02 2015Z,Intel(R) Capability Licensing Service TCP IP
Interface,Intel(R) Capability Licensing Service TCP IP Interface,"C:\Program
Files\Intel\TXE Components\TCS\SocketHeciServer.exe",,Manual,****LocalSystem
Thu Aug 13 22:13:17
2015Z,HdAudAddService,@hdaudio.inf;%UAAFunctionDriverForHdAudio.SvcDesc%;Microsoft
1.1 UAA Function Driver for High Definition Audio
Service,\SystemRoot\system32\DRIVERS\HdAudio.sys,,Manual,
Thu Aug 13 22:06:38 2015Z,ClipSVC\Parameters,,%SystemRoot%\System32\ClipSVC.dll,,,
Thu Aug 13 21:56:11
2015Z,WlanSvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Thu Aug 13 21:55:42 2015Z,acpipagr,@acpipagr.inf;%SvcDesc%;ACPI Processor Aggregator
Driver,\SystemRoot\System32\drivers\acpipagr.sys,,Manual,
Thu Aug 13 21:55:42
2015Z,iaLPSSi_GPIO,@ialpssi_gpio.inf;%iaLPSSi_GPIO.SVCDESC%;Intel(R) Serial IO GPIO
Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_GPIO.sys,,Manual,
Thu Aug 13 21:55:42
2015Z,iaLPSSi_I2C,@ialpssi_i2c.inf;%iaLPSSi_I2C.SVCDESC%;Intel(R) Serial IO I2C
Controller Driver,\SystemRoot\System32\drivers\iaLPSSi_I2C.sys,,Manual,
Thu Aug 13 21:55:42
2015Z,TPM,@tpm.inf;%TPM%;TPM,\SystemRoot\system32\drivers\tpm.sys,,Manual,
Thu Aug 13 21:54:58 2015Z,SecureLine,Avast SecureLine,C:\Program Files\AVAST
Software\SecureLine\VpnSvc.exe,,Auto Start,****LocalSystem
Thu Aug 13 21:54:41 2015Z,3ware,,System32\drivers\3ware.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,ADP80XX,,System32\drivers\ADP80XX.SYS,,Boot Start,
Thu Aug 13 21:54:41 2015Z,agp440,@machine.inf;%agp440_svcdesc%;Intel AGP Bus
Filter,System32\drivers\agp440.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,amdsata,,System32\drivers\amdsata.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,amdsbs,,System32\drivers\amdsbs.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,amdxata,,System32\drivers\amdxata.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,arcsas,@arcsas.inf;%arcsas_ServiceName%;Adaptec
SAS/SATA-II RAID Storport's Miniport Driver,System32\drivers\arcsas.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,atapi,@mshdc.inf;%idechannel.DeviceDesc%;IDE
Channel,System32\drivers\atapi.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,b06bdrv,@netbvbda.inf;%vbd_srv_desc%;Broadcom NetXtreme II
VBD,System32\drivers\bxvbda.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,ebdrv,@netevbda.inf;%vbd_srv_desc%;QLogic 10 Gigabit
Ethernet Adapter VBD,System32\drivers\evbda.sys,,Boot Start,
Thu Aug 13 21:54:41
2015Z,EhStorTcgDrv,@ehstortcgdrv.inf;%EhStorTcgDrv.Desc%;Microsoft driver for
storage devices supporting IEEE 1667 and TCG
protocols,System32\drivers\EhStorTcgDrv.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,gagp30kx,@machine.inf;%gagp30kx_svcdesc%;Microsoft Generic
AGPv3.0 Filter for K8 Processor Platforms,System32\drivers\gagp30kx.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,HpSAMD,,System32\drivers\HpSAMD.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,iaStorAV,@iastorav.inf;%iaStorAV.DeviceDesc%;Intel(R) SATA
RAID Controller Windows,System32\drivers\iaStorAV.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,iaStorV,@iastorv.inf;%*PNP0600.DeviceDesc%;Intel RAID
Controller Windows 7,System32\drivers\iaStorV.sys,,Boot Start,
Page 165

SYSTEM OUTPUT.txt
Thu Aug 13 21:54:41 2015Z,intelide,,System32\drivers\intelide.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,isapnp,,System32\drivers\isapnp.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS,,System32\drivers\lsi_sas.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS2i,,System32\drivers\lsi_sas2i.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SAS3i,,System32\drivers\lsi_sas3i.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,LSI_SSS,,System32\drivers\lsi_sss.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,megasas,,System32\drivers\megasas.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,megasr,,System32\drivers\megasr.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,mvumis,,System32\drivers\mvumis.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,nvraid,,System32\drivers\nvraid.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,nvstor,,System32\drivers\nvstor.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,nv_agp,@machine.inf;%agpnvidia_svcdesc%;NVIDIA nForce AGP
Bus Filter,System32\drivers\nv_agp.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,pciide,,System32\drivers\pciide.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,pcmcia,,System32\drivers\pcmcia.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,percsas2i,,System32\drivers\percsas2i.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,percsas3i,,System32\drivers\percsas3i.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,sbp2port,@sbp2.inf;%sbp2_ServiceDesc%;SBP-2
Transport/Protocol Bus Driver,System32\drivers\sbp2port.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,SiSRaid2,,System32\drivers\SiSRaid2.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,SiSRaid4,,System32\drivers\sisraid4.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,stexstor,,System32\drivers\stexstor.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,storflt,@wstorflt.inf;%service_desc%;Microsoft Hyper-V
Storage Accelerator,System32\drivers\vmstorfl.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,storufs,@storufs.inf;%UfsServiceDesc%;Microsoft Universal
Flash Storage (UFS) Driver,System32\drivers\storufs.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,storvsc,,System32\drivers\storvsc.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,uagp35,@machine.inf;%uagp35_svcdesc%;Microsoft AGPv3.5
Filter,System32\drivers\uagp35.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,uliagpkx,@machine.inf;%uliagpkx_svcdesc%;Uli AGP Bus
Filter,System32\drivers\uliagpkx.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,vmbus,@wvmbus.inf;%vmbus.SVCDESC%;Virtual Machine
Bus,System32\drivers\vmbus.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,vsmraid,,System32\drivers\vsmraid.sys,,Boot Start,
Thu Aug 13 21:54:41 2015Z,VSTXRAID,@vstxraid.inf;%Driver.DeviceDesc%;VIA StorX
Storage RAID Controller Windows Driver,System32\drivers\vstxraid.sys,,Boot Start,
Thu Jul 16 04:12:19 2015Z,WINUSB,@winusb.inf;%WINUSB_SvcDesc%;WinUsb
Driver,\SystemRoot\System32\drivers\WinUSB.SYS,,Manual,
Thu Jul 16 04:12:16 2015Z,terminpt,@termmou.inf;%TermInpt.SVCDESC%;Microsoft Remote
Desktop Input Driver,\SystemRoot\System32\drivers\terminpt.sys,,Manual,
Thu Jul 16 04:12:01 2015Z,kbdhid,@keyboard.inf;%KBDHID.SvcDesc%;Keyboard HID
Driver,\SystemRoot\System32\drivers\kbdhid.sys,,Manual,
Thu Jul 16 04:11:59 2015Z,WUDFRd,@hidbthle.inf;%wudfRdDisplayName%;Windows Driver
Foundation - User-mode Driver Framework
Reflector,\SystemRoot\System32\drivers\WUDFRd.sys,,Manual,
Thu Jul 16 04:01:46
2015Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Thu Jul 16 03:47:02 2015Z,UEIPSvc,User Experience Improvement Program,"C:\Program
Files\Acer\User Experience Improvement
Program\Framework\UBTService.exe",,Manual,****LocalSystem
Thu Jul 16 03:46:19 2015Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program
Files (x86)\Mozilla Maintenance
Service\maintenanceservice.exe",,Manual,****LocalSystem
Thu Jul 16 03:44:48
2015Z,GamesAppIntegrationService,GamesAppIntegrationService,"C:\Program Files
(x86)\WildTangent Games\App\GamesAppIntegrationService.exe",,Auto
Start,****LocalSystem
Thu Jul 16 03:44:47 2015Z,GamesAppService,GamesAppService,"C:\Program Files
(x86)\WildTangent Games\App\GamesAppService.exe",,Manual,****LocalSystem
Thu Jul 16 03:41:07
2015Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot
%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,,Manual,****NT
Page 166

SYSTEM OUTPUT.txt

Authority\LocalService
Thu Jul 16 03:40:55 2015Z,.NET CLR Data,,,^^^^,,
Thu Jul 16 03:40:55 2015Z,.NET CLR Networking,,,^^^^,,
Thu Jul 16 03:40:55 2015Z,clr_optimization_v2.0.50727_32,,,^^^^,,
Thu Jul 16 03:40:55 2015Z,clr_optimization_v2.0.50727_64,,,^^^^,,
Thu Jul 16 03:34:32
2015Z,PrintNotify,@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll;-1,%Syste
mRoot%\system32\svchost.exe -k print,^^^^288,3,LocalSystem
Thu Jul 16 03:34:32
2015Z,PrintNotify\Parameters,,C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dl
l,,,
Thu Jul 16 03:32:47 2015Z,WlanSvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,
Thu Jul 16 03:32:44
2015Z,NativeWifiP,@%SystemRoot%\System32\drivers\nwifi.sys;-101,system32\DRIVERS\nwi
fi.sys,,Manual,
Thu Jul 16 03:31:44 2015Z,GPIOClx0101,Microsoft GPIO Class Extension
Driver,System32\Drivers\msgpioclx.sys,,Manual,
Thu Jul 16 03:31:44 2015Z,SpbCx,Simple Peripheral Bus Support
Library,system32\drivers\SpbCx.sys,,Manual,
Fri Jul 10 13:19:52
2015Z,NgcCtnrSvc\Parameters,,%SystemRoot%\System32\NgcCtnrSvc.dll,,,
Fri Jul 10 13:19:52 2015Z,VaultSvc\Parameters,,C:\Windows\System32\vaultsvc.dll,,,
Fri Jul 10 13:14:47
2015Z,RDPDR,@%SystemRoot%\System32\DRIVERS\rdpdr.sys;-100,System32\drivers\rdpdr.sys
,,Manual,
Fri Jul 10 13:14:47 2015Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,,Manual,
Fri Jul 10 13:14:47
2015Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svcho
st.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 13:14:47
2015Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Fri Jul 10 13:14:46 2015Z,RDPUDD,,,^^^^,,
Fri Jul 10 13:14:46 2015Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,
Fri Jul 10 13:14:46
2015Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,
Fri Jul 10 12:22:48
2015Z,Synth3dVsc,,\SystemRoot\System32\drivers\Synth3dVsc.sys,,Manual,
Fri Jul 10 12:22:47 2015Z,dmvsc,,\SystemRoot\System32\drivers\dmvsc.sys,,Manual,
Fri Jul 10 12:22:47 2015Z,gencounter,@wgencounter.inf;%GenCounter.SVCDESC%;Microsoft
Hyper-V Generation Counter,\SystemRoot\System32\drivers\vmgencounter.sys,,Manual,
Fri Jul 10 12:22:44 2015Z,UASPStor,@uaspstor.inf;%UASPortName%;USB Attached SCSI
(UAS) Driver,\SystemRoot\System32\drivers\uaspstor.sys,,Manual,
Fri Jul 10 12:22:43 2015Z,sdstor,@sdstor.inf;%sdstor_ServiceDesc%;SD Storage Port
Driver,\SystemRoot\System32\drivers\sdstor.sys,,Manual,
Fri Jul 10 12:22:41 2015Z,npsvctrig,@npsvctrig.inf;%NPSVCTRIG.SvcDisplayName%;Named
pipe service trigger provider,\SystemRoot\System32\drivers\npsvctrig.sys,,System
Start,
Fri Jul 10 12:22:39
2015Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,\SystemRoot\System32\drivers
\asyncmac.sys,,Manual,
Fri Jul 10 12:22:25 2015Z,IPMIDRV,,\SystemRoot\System32\drivers\IPMIDrv.sys,,Manual,
Fri Jul 10 12:22:25 2015Z,iScsiPrt,@iscsi.inf;%iScsiPortName%;iScsiPort
Driver,\SystemRoot\System32\drivers\msiscsi.sys,,Manual,
Fri Jul 10 12:22:22 2015Z,HidBatt,@hidbatt.inf;%HidBatt.SvcDesc%;HID UPS Battery
Driver,\SystemRoot\System32\drivers\HidBatt.sys,,Manual,
Fri Jul 10 12:22:22
2015Z,mshidumdf,@%SystemRoot%\system32\drivers\mshidumdf.sys;-100,\SystemRoot\System
32\drivers\mshidumdf.sys,,Manual,
Fri Jul 10 12:22:21 2015Z,fdc,@fdc.inf;%fdc_ServiceDesc%;Floppy Disk Controller
Driver,\SystemRoot\System32\drivers\fdc.sys,,Manual,
Fri Jul 10 12:22:21 2015Z,flpydisk,@flpydisk.inf;%floppy_ServiceDesc%;Floppy Disk
Page 167

SYSTEM OUTPUT.txt
Driver,\SystemRoot\System32\drivers\flpydisk.sys,,Manual,
Fri Jul 10 12:22:21 2015Z,sfloppy,@flpydisk.inf;%sfloppy_devdesc%;High-Capacity
Floppy Disk Drive,\SystemRoot\System32\drivers\sfloppy.sys,,Manual,
Fri Jul 10 12:22:20 2015Z,CapImg,@capimg.inf;%CapImgHid_Service%;HID driver for
CapImg touch screen,\SystemRoot\System32\drivers\capimg.sys,,Manual,
Fri Jul 10 12:22:19 2015Z,BTHMODEM,@bthspp.inf;%BthSerial.DisplayName%;Bluetooth
Serial Communications Driver,\SystemRoot\System32\drivers\bthmodem.sys,,Manual,
Fri Jul 10 12:22:18 2015Z,bthhfhid,@bthaudhid.inf;%BthAudioHFHid.SVCDESC%;Bluetooth
Hands-Free Call Control HID,\SystemRoot\System32\drivers\BthHFHid.sys,,Manual,
Fri Jul 10 12:22:16 2015Z,1394ohci,@1394.inf;%PCI\CC_0C0010.DeviceDesc%;1394 OHCI
Compliant Host Controller,\SystemRoot\System32\drivers\1394ohci.sys,,Manual,
Fri Jul 10 12:22:16 2015Z,AcpiPmi,@acpipmi.inf;%AcpiPmi.SvcDesc%;ACPI Power Meter
Driver,\SystemRoot\System32\drivers\acpipmi.sys,,Manual,
Fri Jul 10 12:22:08
2015Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost
.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 12:21:44
2015Z,iphlpsvc,@%SystemRoot%\system32\iphlpsvc.dll;-500,%SystemRoot%\System32\svchos
t.exe -k NetSvcs,,Auto Start,****LocalSystem
Fri Jul 10 12:21:44
2015Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 12:21:43 2015Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,,<<<<Auto Start,
Fri Jul 10 12:21:43 2015Z,srvnet,,System32\DRIVERS\srvnet.sys,,Manual,
Fri Jul 10 12:21:42
2015Z,MsLldp,@%SystemRoot%\system32\drivers\mslldp.sys;-200,system32\drivers\mslldp.
sys,,<<<<Auto Start,
Fri Jul 10 12:21:37 2015Z,crypt32,,,^^^^,,
Fri Jul 10 12:21:24
2015Z,hyperkbd,,\SystemRoot\System32\drivers\hyperkbd.sys,,Manual,
Fri Jul 10 12:21:24
2015Z,HyperVideo,,\SystemRoot\system32\DRIVERS\HyperVideo.sys,,Manual,
Fri Jul 10 12:21:24 2015Z,netvsc,,\SystemRoot\System32\drivers\netvsc.sys,,Manual,
Fri Jul 10 12:21:24 2015Z,s3cap,,\SystemRoot\System32\drivers\vms3cap.sys,,Manual,
Fri Jul 10 12:21:24
2015Z,VMBusHID,,\SystemRoot\System32\drivers\VMBusHID.sys,,Manual,
Fri Jul 10 12:21:21
2015Z,cnghwassist,@%SystemRoot%\system32\drivers\cnghwassist.sys;-100,System32\DRIVE
RS\cnghwassist.sys,,Disabled,
Fri Jul 10 12:20:51 2015Z,NETVSCVFPP,,,^^^^,,
Fri Jul 10 12:20:44
2015Z,NetSetupSvc,@%SystemRoot%\system32\NetSetupSvc.dll;-3,%SystemRoot%\System32\sv
chost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 12:20:30
2015Z,Psched,@%windir%\System32\drivers\pacer.sys;-101,System32\drivers\pacer.sys,,S
ystem Start,
Fri Jul 10 12:20:30
2015Z,vwififlt,@%SystemRoot%\System32\drivers\vwififlt.sys;-259,System32\drivers\vwi
fiflt.sys,,System Start,
Fri Jul 10 12:20:26
2015Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,,B
oot Start,
Fri Jul 10 12:20:26 2015Z,Tcpip6,@todo.dll;-100;Microsoft IPv6 Protocol
Driver,System32\drivers\tcpip.sys,,Manual,
Fri Jul 10 12:20:26 2015Z,TCPIP6TUNNEL,,,^^^^,,
Fri Jul 10 12:20:26 2015Z,TCPIPTUNNEL,,,^^^^,,
Fri Jul 10 12:20:26
2015Z,WFPLWFS,@%SystemRoot%\System32\drivers\wfplwfs.sys;-6000,System32\drivers\wfpl
wfs.sys,,Boot Start,
Fri Jul 10 12:20:23 2015Z,acpiex,Microsoft ACPIEx
Driver,System32\Drivers\acpiex.sys,,Boot Start,
Fri Jul 10 12:20:23 2015Z,Ucx01000,USB Host Support
Library,system32\drivers\ucx01000.sys,,Manual,
Page 168

SYSTEM OUTPUT.txt
Fri Jul 10 12:20:23 2015Z,WindowsTrustedRT,Windows Trusted Execution Environment
Class Extension,system32\drivers\WindowsTrustedRT.sys,,Boot Start,
Fri Jul 10 12:20:23
2015Z,WindowsTrustedRTProxy,@WindowsTrustedRTProxy.inf;%WindowsTrustedRTProxy.SVCDES
C%;Microsoft Windows Trusted Runtime Secure
Service,System32\drivers\WindowsTrustedRTProxy.sys,,Boot Start,
Fri Jul 10 11:06:22
2015Z,AudioEndpointBuilder,@%SystemRoot%\system32\AudioEndpointBuilder.dll;-204,%Sys
temRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,,Auto
Start,****LocalSystem
Fri Jul 10 11:06:22
2015Z,Audiosrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:06:22
2015Z,MMCSS,@%systemroot%\system32\drivers\mmcss.sys;-100,\SystemRoot\system32\drive
rs\mmcss.sys,,<<<<Auto Start,
Fri Jul 10 11:06:01 2015Z,Winsock,,,^^^^,,
Fri Jul 10 11:05:46
2015Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32
\svchost.exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:46
2015Z,NdisImPlatform,@%SystemRoot%\System32\drivers\ndisimplatform.sys;-501,System32
\drivers\NdisImPlatform.sys,,Manual,
Fri Jul 10 11:05:46
2015Z,NetBIOS,@%windir%\system32\drivers\netbios.sys;-503,system32\drivers\netbios.s
ys,,System Start,
Fri Jul 10 11:05:46 2015Z,NetbiosSmb,,,^^^^,,
Fri Jul 10 11:05:46 2015Z,RDMANDK,,,^^^^,,
Fri Jul 10 11:05:25
2015Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\
afd.sys,,System Start,
Fri Jul 10 11:05:25
2015Z,ahcache,@%systemroot%\system32\drivers\ahcache.sys;-102,system32\DRIVERS\ahcac
he.sys,,System Start,
Fri Jul 10 11:05:25
2015Z,AJRouter,@%SystemRoot%\system32\AJRouter.dll;-2,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,,Manual,
****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,AppID,@%systemroot%\system32\srpapi.dll;-100,\SystemRoot\system32\drivers\appi
d.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceNetworkRestricted,,Manual,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,AppReadiness,@%SystemRoot%\System32\AppReadiness.dll;-1000,%SystemRoot%\System
32\svchost.exe -k AppReadiness,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,AppXSvc,@%SystemRoot%\system32\appxdeploymentserver.dll;-1,%systemroot%\system
32\svchost.exe -k wsappx,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchos
t.exe -k AxInstSVGroup,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25 2015Z,Beep,Beep,,,System Start,
Fri Jul 10 11:05:25

Page 169

SYSTEM OUTPUT.txt
2015Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k
LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,bowser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\bowser.sys,,Ma
nual,
Fri Jul 10 11:05:25
2015Z,BrokerInfrastructure,@%windir%\system32\bisrv.dll;-100,%SystemRoot%\system32\s
vchost.exe -k DcomLaunch,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.
exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,,Disabled,
Fri Jul 10 11:05:25
2015Z,CDPSvc,@%SystemRoot%\system32\cdpsvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,CLFS,@%SystemRoot%\system32\drivers\clfs.sys;-100,System32\drivers\CLFS.sys,,B
oot Start,
Fri Jul 10 11:05:25
2015Z,ClipSVC,@%SystemRoot%\system32\ClipSVC.dll;-103,%SystemRoot%\System32\svchost.
exe -k wsappx,,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,CNG,,System32\Drivers\cng.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,condrv,Console Driver,System32\drivers\condrv.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,CoreMessagingRegistrar,@%SystemRoot%\system32\coremessaging.dll;-1,%SystemRoot
%\system32\svchost.exe -k LocalServiceNoNetwork,,Auto Start,****NT
AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k NetworkService,,Auto Start,****NT Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,dam,@%SystemRoot%\system32\drivers\dam.sys;-100,system32\drivers\dam.sys,,Syst
em Start,
Fri Jul 10 11:05:25
2015Z,DcomLaunch,@combase.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,DcpSvc,@%SystemRoot%\system32\dcpsvc.dll;-3001,%SystemRoot%\System32\svchost.e
xe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svch
ost.exe -k defragsvc,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,DeviceInstall,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\s
vchost.exe -k DcomLaunch,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,DevQueryBroker,@%SystemRoot%\system32\DevQueryBroker.dll;-100,%SystemRoot%\sys
tem32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Dfsc,@%systemroot%\system32\wkssvc.dll;-1008,System32\Drivers\dfsc.sys,,System
Start,
Fri Jul 10 11:05:25
2015Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
Page 170

SYSTEM OUTPUT.txt
e -k LocalServiceNetworkRestricted,,Auto Start,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,diagnosticshub.standardcollector.service,@%SystemRoot%\system32\DiagSvcs\Diagn
osticsHub.StandardCollector.ServiceRes.dll;-1000,%SystemRoot%\system32\DiagSvcs\Diag
nosticsHub.StandardCollector.Service.exe,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,DiagTrack,@%SystemRoot%\system32\diagtrack.dll;-3001,%SystemRoot%\System32\svc
host.exe -k utcsvc,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,DmEnrollmentSvc,@%systemroot%\system32\Windows.Internal.Management.dll;-100,%s
ystemroot%\system32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,dmwappushservice,@%SystemRoot%\system32\dmwappushsvc.dll;-200,%SystemRoot%\sys
tem32\svchost.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,DoSvc,@%systemroot%\system32\dosvc.dll;-100,%systemroot%\system32\svchost.exe
-k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,DsmSvc,@%SystemRoot%\system32\DeviceSetupManager.dll;-1000,%SystemRoot%\system
32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,DsSvc,@%SystemRoot%\system32\dssvc.dll;-10003,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,Eaphost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,,Ma
nual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,embeddedmode,@%SystemRoot%\system32\embeddedmodesvc.dll;-200,%SystemRoot%\Syst
em32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,EntAppSvc,@EnterpriseAppMgmtSvc.dll;-1,%systemroot%\system32\svchost.exe -k
appmodel,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,exfat,exFAT File System Driver,,,Manual,
Fri Jul 10 11:05:25 2015Z,fastfat,FAT12/16/32 File System Driver,,,Manual,
Fri Jul 10 11:05:25
2015Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,,
Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\System32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,fhsvc,@%systemroot%\system32\fhsvc.dll;-101,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Page 171

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,FileCrypt,@%systemroot%\system32\drivers\filecrypt.sys;-100,system32\drivers\f
ilecrypt.sys,,System Start,
Fri Jul 10 11:05:25
2015Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,System32\drivers\fil
einfo.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmg
r.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho
st.exe -k LocalService,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers
\FsDepends.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,Fs_Rec,,,^^^^8,0,
Fri Jul 10 11:05:25 2015Z,gpsvc,@gpapi.dll;-112,%systemroot%\system32\svchost.exe -k
netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,GpuEnergyDrv,@%SystemRoot%\system32\drivers\gpuenergydrv.sys;-100,System32\dri
vers\gpuenergydrv.sys,,System Start,
Fri Jul 10 11:05:25
2015Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalServiceNetworkRestricted,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,,Man
ual,
Fri Jul 10 11:05:25
2015Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwp
olicy.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,icssvc,@%SystemRoot%\System32\tetheringservice.dll;-4097,%SystemRoot%\system32
\svchost.exe -k LocalServiceNetworkRestricted,,Manual,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%Syst
emRoot%\system32\IEEtwCollector.exe /V,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,IoQos,@%SystemRoot%\system32\drivers\ioqos.sys;-100,system32\drivers\ioqos.sys
,,Manual,
Fri Jul 10 11:05:25
2015Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt
drv.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.
sys,,Manual,
Fri Jul 10 11:05:25
2015Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,,Manual,****LocalSyste
m
Fri Jul 10 11:05:25 2015Z,KSecDD,,System32\Drivers\ksecdd.sys,,Boot Start,
Fri Jul 10 11:05:25 2015Z,KSecPkg,,System32\Drivers\ksecpkg.sys,,Boot Start,
Fri Jul 10 11:05:25 2015Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,,Manual,****NT AUTHORITY\NetworkService
Page 172

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:25
2015Z,lfsvc,@%SystemRoot%\System32\lfsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,LicenseManager,@%SystemRoot%\system32\licensemanagersvc.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalService,,Manual,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,LSM,@%windir%\system32\lsm.dll;-1001,%SystemRoot%\system32\svchost.exe -k DcomLaunch,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drivers\luafv.sys,,<<<<Auto Start,
Fri Jul 10 11:05:25
2015Z,MapsBroker,@%SystemRoot%\System32\moshost.dll;-100,%SystemRoot%\System32\svchost.exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,Modem,,system32\drivers\modem.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mountmgr.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,mpsdrv,@%SystemRoot%\system32\drivers\mpsdrv.sys;-23092,System32\drivers\mpsdrv.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork,,Auto Start,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mrxdav.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys,,<<<<Auto Start,
Fri Jul 10 11:05:25
2015Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.exe /V,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,NcaSvc,@%SystemRoot%\system32\ncasvc.dll;-3009,%SystemRoot%\System32\svchost.exe -k NetSvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,NcbService,@%SystemRoot%\system32\ncbservice.dll;-500,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,NcdAutoSetup,@%SystemRoot%\system32\NcdAutoSetup.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,,B

Page 173

SYSTEM OUTPUT.txt

oot Start,
Fri Jul 10 11:05:25
2015Z,NdisCap,@%SystemRoot%\System32\drivers\ndiscap.sys;-5000,System32\drivers\ndis
cap.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,Ndu,@%SystemRoot%\system32\drivers\Ndu.sys;-10001,system32\drivers\Ndu.sys,,<<
<<Auto Start,
Fri Jul 10 11:05:25
2015Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,,
System Start,
Fri Jul 10 11:05:25
2015Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.
exe,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,netprofm,@%SystemRoot%\system32\netprofmsvc.dll;-202,%SystemRoot%\System32\svc
host.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NetTcpPortSharing,@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceMo
delInstallRC.dll;-8201,%systemroot%\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.e
xe,,Disabled,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NgcCtnrSvc,@%SystemRoot%\System32\NgcCtnrSvc.dll;-1,%SystemRoot%\system32\svch
ost.exe -k LocalServiceNetworkRestricted,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,NgcSvc,@%SystemRoot%\System32\ngcsvc.dll;-100,%SystemRoot%\system32\lsass.exe,
,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,,Auto Start,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsipr
oxy.sys,,System Start,
Fri Jul 10 11:05:25 2015Z,NTFS,,,,Manual,
Fri Jul 10 11:05:25
2015Z,OneSyncSvc,@%SystemRoot%\system32\APHostRes.dll;-10002,%SystemRoot%\system32\s
vchost.exe -k UnistackSvcGroup,^^^^96,2,LocalSystem
Fri Jul 10 11:05:25
2015Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25 2015Z,pcw,Performance Counters for Windows
Driver,System32\drivers\pcw.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,pdc,@%SystemRoot%\system32\drivers\pdc.sys;-100,system32\drivers\pdc.sys,,Boot
Start,
Fri Jul 10 11:05:25
2015Z,PerfHost,@%systemroot%\sysWow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PimIndexMaintenanceSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-15001,%Sy
stemRoot%\system32\svchost.exe -k UnistackSvcGroup,^^^^96,3,LocalSystem
Fri Jul 10 11:05:25

Page 174

SYSTEM OUTPUT.txt

2015Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-200,%SystemRoot%\system32\svchos
t.exe -k DcomLaunch,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\sv
chost.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost
.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\sv
chost.exe -k NetworkServiceNetworkRestricted,,Manual,****NT Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.
exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\d
rivers\qwavedrv.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
xe -k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,,Syst
em Start,
Fri Jul 10 11:05:25 2015Z,ReFSv1,,,,Manual,
Fri Jul 10 11:05:25
2015Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,,Disabled,****localSystem
Fri Jul 10 11:05:25
2015Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k
localService,,Disabled,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,RetailDemo,@%SystemRoot%\System32\RDXService.dll;-256,%SystemRoot%\System32\sv
chost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator
.exe,,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,RpcSs,@combase.dll;-5010,%SystemRoot%\system32\svchost.exe
-k rpcss,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,,Au
to Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,,Disabled,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,ScDeviceEnum,@%SystemRoot%\System32\ScDeviceEnum.dll;-100,%SystemRoot%\system3
2\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25

Page 175

SYSTEM OUTPUT.txt
2015Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfi
lter.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.ex
e -k SDRSVC,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.e
xe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SensorDataService,@%SystemRoot%\system32\SensorDataService.exe;-101,%SystemRoo
t%\System32\SensorDataService.exe,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SensorService,@%SystemRoot%\System32\sensorservice.dll;-1000,%SystemRoot%\syst
em32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,SerCx,Serial UART Support
Library,system32\drivers\SerCx.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,SerCx2,Serial UART Support
Library,system32\drivers\SerCx2.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svch
ost.exe -k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\sv
chost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System3
2\svchost.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,smphost,@%SystemRoot%\System32\smphost.dll;-102,%SystemRoot%\System32\svchost.
exe -k smphost,,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,SmsRouter,@%SystemRoot%\System32\SmsRouterSvc.dll;-10001,%SystemRoot%\system32
\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap
.exe,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.ex
e,^^^^272,2,LocalSystem
Fri Jul 10 11:05:25
2015Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe
,,Auto Start,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,srv,@%systemroot%\system32\srvsvc.dll;-102,System32\DRIVERS\srv.sys,,<<<<Auto
Start,
Fri Jul 10 11:05:25
2015Z,srv2,@%systemroot%\system32\srvsvc.dll;-104,System32\DRIVERS\srv2.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT Authority\LocalService
Fri Jul 10 11:05:25
Page 176

SYSTEM OUTPUT.txt

2015Z,StateRepository,@%SystemRoot%\system32\windows.staterepository.dll;-1,%SystemR
oot%\system32\svchost.exe -k appmodel,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,storqosflt,@%SystemRoot%\System32\drivers\storqosflt.sys;-101,system32\drivers
\storqosflt.sys,,<<<<Auto Start,
Fri Jul 10 11:05:25
2015Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,svsvc,@%SystemRoot%\System32\svsvc.dll;-101,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe
-k swprv,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,SystemEventsBroker,@%windir%\system32\SystemEventsBrokerServer.dll;-1001,%Syst
emRoot%\system32\svchost.exe -k DcomLaunch,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchos
t.exe -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,tcpipreg,TCP/IP Registry
Compatibility,System32\drivers\tcpipreg.sys,,<<<<Auto Start,
Fri Jul 10 11:05:25
2015Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,\SystemRoot\system32\DRIVERS\td
x.sys,,System Start,
Fri Jul 10 11:05:25
2015Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,,Manual,****NT Authority\NetworkService
Fri Jul 10 11:05:25
2015Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
host.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,tiledatamodelsvc,@%SystemRoot%\system32\tileobjserver.dll;-1,%systemroot%\syst
em32\svchost.exe -k appmodel,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,TimeBroker,@%windir%\system32\TimeBrokerServer.dll;-1001,%SystemRoot%\system32
\svchost.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Trkwks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,TsUsbFlt,@%SystemRoot%\system32\drivers\tsusbflt.sys;-1000,System32\drivers\Ts
UsbFlt.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,UcmCx0101,USB Connector Manager KMDF Class
Extension,System32\Drivers\UcmCx.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,UdeCx,USB Device Emulation Support
Library,system32\drivers\udecx.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,udfs,udfs,system32\DRIVERS\udfs.sys,,Disabled,
Fri Jul 10 11:05:25 2015Z,Ufx01000,USB Function Class
Extension,system32\drivers\ufx01000.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,UIODetect,@%SystemRoot%\system32\uiOdetect.exe;-101,%SystemRoot%\system32\UIOD
etect.exe,^^^^272,3,LocalSystem
Fri Jul 10 11:05:25
2015Z,UnistoreSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-10003,%SystemRoot%\S
ystem32\svchost.exe -k UnistackSvcGroup,^^^^96,3,LocalSystem
Fri Jul 10 11:05:25
2015Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,UrsCx01000,USB Role-Switch Support

Page 177

SYSTEM OUTPUT.txt
Library,system32\drivers\urscx01000.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,UserDataSvc,@%SystemRoot%\system32\UserDataAccessRes.dll;-14001,%SystemRoot%\s
ystem32\svchost.exe -k UnistackSvcGroup,^^^^96,3,LocalSystem
Fri Jul 10 11:05:25
2015Z,UserManager,@%systemroot%\system32\usermgr.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****LocalSystem
Fri Jul 10 11:05:25
2015Z,UsoSvc,@%systemroot%\system32\usocore.dll;-102,%systemroot%\system32\svchost.e
xe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,,Manual,
****LocalSystem
Fri Jul 10 11:05:25
2015Z,vhf,@%SystemRoot%\system32\drivers\vhf.sys;-100,\SystemRoot\System32\drivers\v
hf.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,vmicguestinterface,@%systemroot%\system32\icsvc.dll;-801,%systemroot%\system32
\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicheartbeat,@%systemroot%\system32\icsvc.dll;-101,%systemroot%\system32\svch
ost.exe -k ICService,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmickvpexchange,@%systemroot%\system32\icsvc.dll;-201,%systemroot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicrdv,@%systemroot%\system32\icsvc.dll;-601,%systemroot%\system32\svchost.ex
e -k ICService,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicshutdown,@%systemroot%\system32\icsvc.dll;-301,%systemroot%\system32\svcho
st.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmictimesync,@%systemroot%\system32\icsvc.dll;-401,%systemroot%\system32\svcho
st.exe -k LocalServiceNetworkRestricted,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,vmicvmsession,@%systemroot%\system32\icsvc.dll;-901,%systemroot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,vmicvss,@%systemroot%\system32\icsvc.dll;-501,%systemroot%\system32\svchost.ex
e -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmg
rx.sys,,Boot Start,
Fri Jul 10 11:05:25
2015Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,,Man
ual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WalletService,@%SystemRoot%\System32\WalletService.dll;-1000,%SystemRoot%\Syst
em32\svchost.exe -k appmodel,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,WbioSrvc,@%systemroot%\system32\wbiosrvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k WbioSvcGroup,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,Wcmsvc,@%SystemRoot%\System32\wcmsvc.dll;-4097,%SystemRoot%\system32\svchost.e
Page 178

SYSTEM OUTPUT.txt
xe -k LocalServiceNetworkRestricted,,Auto Start,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcssvc,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,wdiwifi,WDI Driver
Framework,system32\DRIVERS\wdiwifi.sys,,Manual,
Fri Jul 10 11:05:25 2015Z,WdNisSvc,@%ProgramFiles%\Windows
Defender\MpAsDesc.dll;-320,"%ProgramFiles%\Windows
Defender\NisSrv.exe",,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,WEPHOSTSVC,@%systemroot%\system32\wephostsvc.dll;-100,%systemroot%\system32\sv
chost.exe -k WepHostSvcGroup,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,,Manual,****localSystem
Fri Jul 10 11:05:25
2015Z,WiaRpc,@%SystemRoot%\system32\wiarpc.dll;-2,%SystemRoot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25 2015Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****localSystem
Fri Jul 10 11:05:25
2015Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25
2015Z,wlidsvc,@%SystemRoot%\system32\wlidsvc.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,,Manual,****localSystem
Fri Jul 10 11:05:25 2015Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media
Player\wmpnetwk.exe",,Manual,****NT AUTHORITY\NetworkService
Fri Jul 10 11:05:25 2015Z,Wof,Windows Overlay File System Filter Driver,,,Boot
Start,
Fri Jul 10 11:05:25
2015Z,workfolderssvc,@%systemroot%\system32\workfolderssvc.dll;-102,%SystemRoot%\Sys
tem32\svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25 2015Z,wpcfltr,Family Safety Filter
Driver,system32\DRIVERS\wpcfltr.sys,,Manual,
Fri Jul 10 11:05:25

Page 179

SYSTEM OUTPUT.txt
2015Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,WpnService,@%SystemRoot%\system32\wpnservice.dll;-1,%systemroot%\system32\svch
ost.exe -k wswpnservice,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,ws2ifsl,@%systemroot%\System32\drivers\ws2ifsl.sys;-1000,\SystemRoot\system32\
drivers\ws2ifsl.sys,,Disabled,
Fri Jul 10 11:05:25
2015Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Fri Jul 10 11:05:25
2015Z,WSService,@%SystemRoot%\system32\WSService.dll;-103,%SystemRoot%\System32\svch
ost.exe -k wsappx,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,WudfPf,@%SystemRoot%\system32\drivers\Wudfpf.sys;-1000,system32\drivers\WudfPf
.sys,,Manual,
Fri Jul 10 11:05:25
2015Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalServiceNoNetwork,,Manual,****NT Authority\LocalService
Fri Jul 10 11:05:25
2015Z,XblAuthManager,@%systemroot%\system32\XblAuthManager.dll;-100,%SystemRoot%\sys
tem32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,XblGameSave,@%systemroot%\system32\XblGameSave.dll;-100,%SystemRoot%\system32\
svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:25
2015Z,XboxNetApiSvc,@%systemroot%\system32\XboxNetApiSvc.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Fri Jul 10 11:05:06 2015Z,.NET CLR Networking 4.0.0.0,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,.NET Data Provider for Oracle,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,.NET Data Provider for SqlServer,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,.NET Memory Cache 4.0,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,.NETFramework,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,ADOVMPPackage,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,adsi,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,AJRouter\Parameters,,%SystemRoot%\System32\AJRouter.dll,,,
Fri Jul 10 11:05:06 2015Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,
Fri Jul 10 11:05:06
2015Z,AppReadiness\Parameters,,%SystemRoot%\system32\AppReadiness.dll,,,
Fri Jul 10 11:05:06
2015Z,AppXSvc\Parameters,,%SystemRoot%\system32\appxdeploymentserver.dll,,,
Fri Jul 10 11:05:06
2015Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\AudioEndpointBuilder.dl
l,,,
Fri Jul 10 11:05:06 2015Z,Audiosrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Fri Jul 10 11:05:06 2015Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,
Fri Jul 10 11:05:06 2015Z,BattC,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,
Fri Jul 10 11:05:06 2015Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,
Fri Jul 10 11:05:06 2015Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Fri Jul 10 11:05:06
2015Z,BrokerInfrastructure\Parameters,,%SystemRoot%\System32\bisrv.dll,,,
Fri Jul 10 11:05:06 2015Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,
Fri Jul 10 11:05:06 2015Z,CDPSvc\Parameters,,%SystemRoot%\System32\CDPSvc.dll,,,
Fri Jul 10 11:05:06
2015Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Fri Jul 10 11:05:06 2015Z,clr_optimization_v4.0.30319_32,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,clr_optimization_v4.0.30319_64,,,^^^^,,
Page 180

SYSTEM OUTPUT.txt

Fri Jul 10 11:05:06
2015Z,CoreMessagingRegistrar\Parameters,,%SystemRoot%\system32\coremessaging.dll,,,
Fri Jul 10 11:05:06 2015Z,CoreUI,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,DCLocator,,,^^^^,,
Fri Jul 10 11:05:06 2015Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Fri Jul 10 11:05:06 2015Z,DcpSvc\Parameters,,%SystemRoot%\system32\dcpsvc.dll,,,
Fri Jul 10 11:05:06
2015Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,
Fri Jul 10 11:05:06
2015Z,DeviceAssociationService\Parameters,,%SystemRoot%\system32\das.dll,,,
Fri Jul 10 11:05:06
2015Z,DevQueryBroker\Parameters,,%SystemRoot%\system32\DevQueryBroker.dll,,,
Fri Jul 10 11:05:06 2015Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,
Fri Jul 10 11:05:06
2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,
Fri Jul 10 11:05:06
2015Z,DmEnrollmentSvc\Parameters,,%systemroot%\system32\Windows.Internal.Management.
dll,,,
Fri Jul 10 11:05:06
2015Z,dmwappushservice\Parameters,,%SystemRoot%\system32\dmwappushsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,
Fri Jul 10 11:05:06 2015Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,
Fri Jul 10 11:05:06 2015Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Fri Jul 10 11:05:06
2015Z,DsmSvc\Parameters,,%SystemRoot%\System32\DeviceSetupManager.dll,,,
Fri Jul 10 11:05:06 2015Z,DsSvc\Parameters,,%SystemRoot%\System32\DsSvc.dll,,,
Fri Jul 10 11:05:06 2015Z,Eaphost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Fri Jul 10 11:05:06 2015Z,EFS\Parameters,,%SystemRoot%\system32\efssvc.dll,,,
Fri Jul 10 11:05:06
2015Z,embeddedmode\Parameters,,%SystemRoot%\System32\embeddedmodesvc.dll,,,
Fri Jul 10 11:05:06
2015Z,EntAppSvc\Parameters,,%SystemRoot%\system32\EnterpriseAppMgmtSvc.dll,,,
Fri Jul 10 11:05:06 2015Z,ESENT,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,
Fri Jul 10 11:05:05 2015Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,
Fri Jul 10 11:05:05 2015Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,
Fri Jul 10 11:05:05 2015Z,fhsvc\Parameters,,%SystemRoot%\system32\fhsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,
Fri Jul 10 11:05:05 2015Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,
Fri Jul 10 11:05:05
2015Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,icssvc\Parameters,,%SystemRoot%\System32\tetheringservice.dll,,,
Fri Jul 10 11:05:05 2015Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,
Fri Jul 10 11:05:05 2015Z,inetaccs,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,KeyIso\Parameters,,%SystemRoot%\system32\keyiso.dll,,,
Fri Jul 10 11:05:05 2015Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,
Fri Jul 10 11:05:05
2015Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Fri Jul 10 11:05:05 2015Z,ldap,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,lfsvc\Parameters,,%SystemRoot%\System32\lfsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,LicenseManager\Parameters,,%SystemRoot%\system32\LicenseManagerSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Lsa,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,LSM\Parameters,,%SystemRoot%\System32\lsm.dll,,,
Fri Jul 10 11:05:05

Page 181

SYSTEM OUTPUT.txt

```
2015Z,MapsBroker\Parameters,,%SystemRoot%\System32\moshost.dll,,,
Fri Jul 10 11:05:05 2015Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Msfs,,,,System Start,
Fri Jul 10 11:05:05 2015Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,
Fri Jul 10 11:05:05 2015Z,MsRPC,,,,Manual,
Fri Jul 10 11:05:05 2015Z,MSSCNTRS,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,napagent,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,NcaSvc\Parameters,,%SystemRoot%\System32\ncasvc.dll,,,
Fri Jul 10 11:05:05
2015Z,NcbService\Parameters,,%SystemRoot%\System32\ncbservice.dll,,,
Fri Jul 10 11:05:05
2015Z,NcdAutoSetup\Parameters,,%SystemRoot%\System32\NcdAutoSetup.dll,,,
Fri Jul 10 11:05:05 2015Z,Netlogon\Parameters,,%SystemRoot%\system32\netlogon.dll,,,
Fri Jul 10 11:05:05 2015Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,
Fri Jul 10 11:05:05
2015Z,netprofm\Parameters,,%SystemRoot%\System32\netprofmsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,NetSetupSvc\Parameters,,%SystemRoot%\System32\NetSetupSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NgcSvc\Parameters,,%SystemRoot%\system32\ngcsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Npfs,,,,System Start,
Fri Jul 10 11:05:05 2015Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Fri Jul 10 11:05:05 2015Z,NTDS,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,Null,,,,System Start,
Fri Jul 10 11:05:05
2015Z,OneSyncSvc\Parameters,,%SystemRoot%\System32\APHostService.dll,,,
Fri Jul 10 11:05:05 2015Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PerfDisk,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,PerfNet,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,PerfOS,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,PerfProc,,,^^^^,,
Fri Jul 10 11:05:05
2015Z,PimIndexMaintenanceSvc\Parameters,,%SystemRoot%\System32\PimIndexMaintenance.d
ll,,,
Fri Jul 10 11:05:05 2015Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,
Fri Jul 10 11:05:05 2015Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,
Fri Jul 10 11:05:05
2015Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,
Fri Jul 10 11:05:05 2015Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,PortProxy,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,
Fri Jul 10 11:05:05 2015Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,
Fri Jul 10 11:05:05 2015Z,RasAcd,Remote Access Auto Connection
Driver,System32\DRIVERS\rasacd.sys,,Manual,
Fri Jul 10 11:05:05 2015Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Fri Jul 10 11:05:05 2015Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,^^^^,,
Fri Jul 10 11:05:05
2015Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Fri Jul 10 11:05:05
2015Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,RetailDemo\Parameters,,%SystemRoot%\system32\RDXService.dll,,,
Fri Jul 10 11:05:05
2015Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Fri Jul 10 11:05:05 2015Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Fri Jul 10 11:05:05 2015Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,
Fri Jul 10 11:05:05
2015Z,ScDeviceEnum\Parameters,,%SystemRoot%\System32\ScDeviceEnum.dll,,,
```

Page 182

SYSTEM OUTPUT.txt
Fri Jul 10 11:05:05 2015Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Fri Jul 10 11:05:05 2015Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,
Fri Jul 10 11:05:05 2015Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,
Fri Jul 10 11:05:05 2015Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,
Fri Jul 10 11:05:05
2015Z,SensorService\Parameters,,%SystemRoot%\system32\SensorService.dll,,,
Fri Jul 10 11:05:05
2015Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,
Fri Jul 10 11:05:05
2015Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,
Fri Jul 10 11:05:05
2015Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Fri Jul 10 11:05:05 2015Z,smphost\Parameters,,%Systemroot%\System32\smphost.dll,,,
Fri Jul 10 11:05:05
2015Z,SmsRouter\Parameters,,%SystemRoot%\system32\SmsRouterSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,
Fri Jul 10 11:05:05 2015Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,StateRepository\Parameters,,%SystemRoot%\system32\windows.staterepository.dll,
,,
Fri Jul 10 11:05:05 2015Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Fri Jul 10 11:05:05 2015Z,svsvc\Parameters,,%SystemRoot%\system32\svsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Fri Jul 10 11:05:05 2015Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Fri Jul 10 11:05:05
2015Z,SystemEventsBroker\Parameters,,%SystemRoot%\System32\SystemEventsBrokerServer.
dll,,,
Fri Jul 10 11:05:05
2015Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Fri Jul 10 11:05:05
2015Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Fri Jul 10 11:05:05
2015Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Fri Jul 10 11:05:05
2015Z,tiledatamodelsvc\Parameters,,%SystemRoot%\system32\tileobjserver.dll,,,
Fri Jul 10 11:05:05
2015Z,TimeBroker\Parameters,,%SystemRoot%\System32\TimeBrokerServer.dll,,,
Fri Jul 10 11:05:05 2015Z,Trkwks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Fri Jul 10 11:05:05 2015Z,TSDDD,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,UGatherer,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,UGTHRSVC,,,^^^^,,
Fri Jul 10 11:05:05
2015Z,UnistoreSvc\Parameters,,%SystemRoot%\System32\unistore.dll,,,
Fri Jul 10 11:05:05 2015Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Fri Jul 10 11:05:05
2015Z,UserDataSvc\Parameters,,%SystemRoot%\System32\userdataservice.dll,,,
Fri Jul 10 11:05:05
2015Z,UserManager\Parameters,,%SystemRoot%\System32\usermgr.dll,,,
Fri Jul 10 11:05:05 2015Z,UsoSvc\Parameters,,%systemroot%\system32\usocore.dll,,,
Fri Jul 10 11:05:05
2015Z,VerifierExt,@%SystemRoot%\system32\drivers\VerifierExt.sys;-1000,system32\driv
ers\VerifierExt.sys,,Manual,
Fri Jul 10 11:05:05
2015Z,vmicguestinterface\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmicheartbeat\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmickvpexchange\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,vmicrdv\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05

Page 183

SYSTEM OUTPUT.txt

2015Z,vmicshutdown\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmictimesync\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05
2015Z,vmicvmsession\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,vmicvss\Parameters,,%SystemRoot%\System32\ICSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Fri Jul 10 11:05:05
2015Z,WalletService\Parameters,,%SystemRoot%\system32\WalletService.dll,,,
Fri Jul 10 11:05:05 2015Z,WbioSrvc\Parameters,,%SystemRoot%\System32\wbiosrvc.dll,,,
Fri Jul 10 11:05:05 2015Z,Wcmsvc\Parameters,,%SystemRoot%\System32\wcmsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Fri Jul 10 11:05:05
2015Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Fri Jul 10 11:05:05 2015Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Fri Jul 10 11:05:05 2015Z,WebClient\Parameters,,%SystemRoot%\System32\webcInt.dll,,,
Fri Jul 10 11:05:05 2015Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WEPHOSTSVC\Parameters,,%systemroot%\system32\wephostsvc.dll,,,
Fri Jul 10 11:05:05
2015Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Fri Jul 10 11:05:05 2015Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WiaRpc\Parameters,,%SystemRoot%\System32\wiarpc.dll,,,
Fri Jul 10 11:05:05
2015Z,WinHttpAutoProxySvc\Parameters,,%SystemRoot%\system32\winhttp.dll,,,
Fri Jul 10 11:05:05 2015Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WinSock2,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,wlidsvc\Parameters,,%SystemRoot%\system32\wlidsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WmiApRpl,,,^^^^,,
Fri Jul 10 11:05:05 2015Z,workerdd,,,^^^^,,
Fri Jul 10 11:05:05
2015Z,workfolderssvc\Parameters,,%systemroot%\system32\workfolderssvc.dll,,,
Fri Jul 10 11:05:05
2015Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Fri Jul 10 11:05:05
2015Z,WpnService\Parameters,,%SystemRoot%\system32\WpnService.dll,,,
Fri Jul 10 11:05:05 2015Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WSearchIdxPi,,,^^^^,,
Fri Jul 10 11:05:05
2015Z,WSService\Parameters,,%SystemRoot%\System32\WSService.dll,,,
Fri Jul 10 11:05:05 2015Z,wuauserv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Fri Jul 10 11:05:05 2015Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,
Fri Jul 10 11:05:05
2015Z,XblAuthManager\Parameters,,%SystemRoot%\System32\XblAuthManager.dll,,,
Fri Jul 10 11:05:05
2015Z,XblGameSave\Parameters,,%SystemRoot%\System32\XblGameSave.dll,,,
Fri Jul 10 11:05:05
2015Z,XboxNetApiSvc\Parameters,,%SystemRoot%\system32\XboxNetApiSvc.dll,,,
Fri Jul 10 11:05:05 2015Z,xmlprov,,,^^^^,,
Fri Jul 10 11:04:15
2015Z,TsUsbGD,@tsgenericusbdriver.inf;%TsUsbGD.DeviceDesc.Generic%;Remote Desktop
Generic USB Device,\SystemRoot\System32\drivers\TsUsbGD.sys,,Manual,
Fri Jul 10 11:04:15
2015Z,UrsChipidea,@urschipidea.inf;%UrsChipidea.ServiceName%;Chipidea USB
Role-Switch Driver,\SystemRoot\System32\drivers\urschipidea.sys,,Manual,
Fri Jul 10 11:04:15
2015Z,UrsSynopsys,@urssynopsys.inf;%UrsSynopsys.ServiceName%;Synopsys USB
Role-Switch Driver,\SystemRoot\System32\drivers\urssynopsys.sys,,Manual,
Fri Jul 10 11:04:13 2015Z,vhdmp,,\SystemRoot\System32\drivers\vhdmp.sys,,Manual,
Fri Jul 10 11:04:12 2015Z,AmdK8,@cpu.inf;%AmdK8.SvcDesc%;AMD K8 Processor
Page 184

```
SYSTEM OUTPUT.txt

Driver,\SystemRoot\System32\drivers\amdk8.sys,,Manual,
Fri Jul 10 11:04:12 2015Z,AmdPPM,@cpu.inf;%AmdPPM.SvcDesc%;AMD Processor
Driver,\SystemRoot\System32\drivers\amdppm.sys,,Manual,
Fri Jul 10 11:04:12 2015Z,Processor,@cpu.inf;%Processor.SvcDesc%;Processor
Driver,\SystemRoot\System32\drivers\processor.sys,,Manual,
Fri Jul 10 11:04:11 2015Z,ufxchipidea,@ufxchipidea.inf;%ufxcename%;USB
Chipidea Controller,\SystemRoot\System32\drivers\ufxchipidea.sys,,Manual,
Fri Jul 10 11:04:11 2015Z,ufxsynopsys,@ufxsynopsys.inf;%ufxcename%;USB
Synopsys Controller,\SystemRoot\System32\drivers\ufxsynopsys.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,1bpbus,@ml4_bus.inf;%1bpbus.servicedesc%;Mellanox
InfiniBand Bus/AL (Filter Driver),\SystemRoot\System32\drivers\1bpbus.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,ml4_bus,@ml4_bus.inf;%MLX4BUS.servicedesc%;Mellanox
ConnectX Bus Enumerator,\SystemRoot\System32\drivers\ml4_bus.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,ndfltr,@ml4_bus.inf;%ndfltr.servicedesc%;NetworkDirect
Service,\SystemRoot\System32\drivers\ndfltr.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,sermouse,@msmouse.inf;%sermouse.SvcDesc%;Serial Mouse
Driver,\SystemRoot\System32\drivers\sermouse.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,winmad,@ml4_bus.inf;%winmad.servicedesc%;winmad
Service,\SystemRoot\System32\drivers\winmad.sys,,Manual,
Fri Jul 10 11:04:08 2015Z,winverbs,@ml4_bus.inf;%winverbs.servicedesc%;winverbs
Service,\SystemRoot\System32\drivers\winverbs.sys,,Manual,
Fri Jul 10 11:04:04 2015Z,hidinterrupt,@HID.inf;%HID.SvcDesc%;Common Driver
for HID Buttons implemented with
interrupts,\SystemRoot\System32\drivers\hidinterrupt.sys,,Manual,
Fri Jul 10 11:04:04 2015Z,wacompen,@hiddigi.inf;%WacomPen.SVCDESC%;Wacom Serial Pen
HID Driver,\SystemRoot\System32\drivers\wacompen.sys,,Manual,
Fri Jul 10 11:04:03 2015Z,acpitime,@acpitime.inf;%AcpiTime.SvcDesc%;ACPI Wake Alarm
Driver,\SystemRoot\System32\drivers\acpitime.sys,,Manual,
Fri Jul 10 11:04:03 2015Z,bcmfn2,@bcmfn2.inf;%bcmfn2.SVCDESC%;bcmfn2
Service,\SystemRoot\System32\drivers\bcmfn2.sys,,Manual,
Fri Jul 10 11:04:03 2015Z,ErrDev,@errdev.inf;%ERRDEV.SvcDesc%;Microsoft Hardware
Error Device Driver,\SystemRoot\System32\drivers\errdev.sys,,Manual,
Fri Jul 10 11:04:03
2015Z,genericusbfn,@genericusbfn.inf;%genericusbfn.ServiceName%;Generic USB Function
Class,\SystemRoot\System32\drivers\genericusbfn.sys,,Manual,
Fri Jul 10 11:04:01 2015Z,wfpcapture,@wfpcapture.inf;%WfpCapture_Desc%;Microsoft WFP
Message Capture,\SystemRoot\System32\drivers\wfpcapture.sys,,Manual,
Fri Jul 10 11:04:01 2015Z,xinputhid,@xinputhid.inf;%xinputhid.SvcDesc%;XINPUT HID
Filter Driver,\SystemRoot\System32\drivers\xinputhid.sys,,Manual,
Fri Jul 10 11:04:00 2015Z,usbcir,@usbcir.inf;%usbcir.SVCDESC%;eHome Infrared
Receiver (USBCIR),\SystemRoot\System32\drivers\usbcir.sys,,Manual,
Fri Jul 10 11:03:59 2015Z,circlass,@circlass.inf;%circlass.SVCDESC%;Consumer IR
Devices,\SystemRoot\System32\drivers\circlass.sys,,Manual,
Fri Jul 10 11:03:59 2015Z,HidBth,@hidbth.inf;%HIDBTH.SvcDesc%;Microsoft Bluetooth
HID Miniport,\SystemRoot\System32\drivers\hidbth.sys,,Manual,
Fri Jul 10 11:03:59 2015Z,HidIr,@hidir.inf;%HIDIR.SvcDesc%;Microsoft Infrared HID
Driver,\SystemRoot\System32\drivers\hidir.sys,,Manual,
Fri Jul 10 11:03:58 2015Z,fvsc,,\SystemRoot\System32\drivers\fvsc.sys,,Manual,
Fri Jul 10 11:03:58 2015Z,vpci,@wvpci.inf;%vpci.SVCDESC%;Microsoft Hyper-V Virtual
PCI Bus,\SystemRoot\System32\drivers\vpci.sys,,Manual,
----------------------------------------
svccli v.20130603
(System) Lists Services keys with ServicedIl values

Thu Apr 21 03:00:51 2016Z
BITS -> %SystemRoot%\System32\qmgr.dll

Tue Mar 29 09:29:40 2016Z
DeviceAssociationService -> %SystemRoot%\System32\das.dll

Wed Mar 23 09:48:50 2016Z
BthHFSrv -> %SystemRoot%\System32\BthHFSrv.dll
```

Page 185

SYSTEM OUTPUT.txt

Wed Mar 23 09:25:17 2016Z
   stisvc -> %SystemRoot%\System32\wiaservc.dll

Tue Mar 22 13:18:45 2016Z
   IKEEXT -> %SystemRoot%\System32\ikeext.dll

Thu Aug 13 21:56:11 2015Z
   WlanSvc -> %SystemRoot%\System32\wlansvc.dll

Thu Jul 16 04:01:46 2015Z
   TabletInputService -> %SystemRoot%\System32\TabSvc.dll

Thu Jul 16 03:34:32 2015Z
   PrintNotify -> C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll

Fri Jul 10 13:14:47 2015Z
   SensrSvc -> %SystemRoot%\system32\sensrsvc.dll
   UmRdpService -> %SystemRoot%\System32\umrdp.dll

Fri Jul 10 12:22:08 2015Z
   wuauserv -> %systemroot%\system32\wuaueng.dll

Fri Jul 10 12:21:44 2015Z
   iphlpsvc -> %SystemRoot%\System32\iphlpsvc.dll
   LanmanServer -> %SystemRoot%\system32\srvsvc.dll

Fri Jul 10 12:20:44 2015Z
   NetSetupSvc -> %SystemRoot%\System32\NetSetupSvc.dll

Fri Jul 10 11:06:22 2015Z
   AudioEndpointBuilder -> %SystemRoot%\System32\AudioEndpointBuilder.dll
   Audiosrv -> %SystemRoot%\System32\Audiosrv.dll

Fri Jul 10 11:05:46 2015Z
   LanmanWorkstation -> %SystemRoot%\System32\wkssvc.dll

Fri Jul 10 11:05:25 2015Z
   AJRouter -> %SystemRoot%\System32\AJRouter.dll
   AppIDSvc -> %SystemRoot%\System32\appidsvc.dll
   Appinfo -> %SystemRoot%\System32\appinfo.dll
   AppReadiness -> %SystemRoot%\system32\AppReadiness.dll
   AppXSvc -> %SystemRoot%\system32\appxdeploymentserver.dll
   AxInstSV -> %SystemRoot%\System32\AxInstSV.dll
   BDESVC -> %SystemRoot%\System32\bdesvc.dll
   BFE -> %SystemRoot%\System32\bfe.dll
   BrokerInfrastructure -> %SystemRoot%\System32\bisrv.dll
   Browser -> %SystemRoot%\System32\browser.dll
   bthserv -> %SystemRoot%\system32\bthserv.dll
   CDPSvc -> %SystemRoot%\System32\CDPSvc.dll
   CertPropSvc -> %SystemRoot%\System32\certprop.dll
   ClipSVC -> %SystemRoot%\System32\ClipSVC.dll
   CoreMessagingRegistrar -> %SystemRoot%\system32\coremessaging.dll
   CryptSvc -> %SystemRoot%\system32\cryptsvc.dll
   DcomLaunch -> %SystemRoot%\system32\rpcss.dll
   DcpSvc -> %SystemRoot%\system32\dcpsvc.dll
   defragsvc -> %Systemroot%\System32\defragsvc.dll
   DeviceInstall -> %SystemRoot%\system32\umpnpmgr.dll
   DevQueryBroker -> %SystemRoot%\system32\DevQueryBroker.dll
   Dhcp -> %SystemRoot%\system32\dhcpcore.dll
   DiagTrack -> %SystemRoot%\system32\diagtrack.dll
   DmEnrollmentSvc -> %systemroot%\system32\Windows.Internal.Management.dll
   dmwappushservice -> %SystemRoot%\system32\dmwappushsvc.dll
   Dnscache -> %SystemRoot%\System32\dnsrslvr.dll
Page 186

```
                              SYSTEM OUTPUT.txt
dot3svc -> %SystemRoot%\System32\dot3svc.dll
DPS -> %SystemRoot%\system32\dps.dll
DsmSvc -> %SystemRoot%\System32\DeviceSetupManager.dll
DsSvc -> %SystemRoot%\System32\DsSvc.dll
Eaphost -> %SystemRoot%\System32\eapsvc.dll
EFS -> %SystemRoot%\system32\efssvc.dll
embeddedmode -> %SystemRoot%\System32\embeddedmodesvc.dll
EntAppSvc -> %SystemRoot%\system32\EnterpriseAppMgmtSvc.dll
EventSystem -> %systemroot%\system32\es.dll
fdPHost -> %SystemRoot%\system32\fdPHost.dll
FDResPub -> %SystemRoot%\system32\fdrespub.dll
fhsvc -> %SystemRoot%\system32\fhsvc.dll
FontCache -> %SystemRoot%\system32\FntCache.dll
gpsvc -> %SystemRoot%\System32\gpsvc.dll
hidserv -> %SystemRoot%\system32\hidserv.dll
HomeGroupListener -> %SystemRoot%\system32\ListSvc.dll
HomeGroupProvider -> %SystemRoot%\system32\provsvc.dll
icssvc -> %SystemRoot%\System32\tetheringservice.dll
KeyIso -> %SystemRoot%\system32\keyiso.dll
KtmRm -> %systemroot%\system32\msdtckrm.dll
lfsvc -> %SystemRoot%\System32\lfsvc.dll
LicenseManager -> %SystemRoot%\system32\LicenseManagerSvc.dll
lltdsvc -> %SystemRoot%\System32\lltdsvc.dll
lmhosts -> %SystemRoot%\System32\lmhsvc.dll
LSM -> %SystemRoot%\System32\lsm.dll
MapsBroker -> %SystemRoot%\System32\moshost.dll
MpsSvc -> %SystemRoot%\system32\mpssvc.dll
MSiSCSI -> %systemroot%\system32\iscsiexe.dll
NcaSvc -> %SystemRoot%\System32\ncasvc.dll
NcbService -> %SystemRoot%\System32\ncbservice.dll
NcdAutoSetup -> %SystemRoot%\System32\NcdAutoSetup.dll
Netlogon -> %SystemRoot%\system32\netlogon.dll
Netman -> %SystemRoot%\System32\netman.dll
netprofm -> %SystemRoot%\System32\netprofmsvc.dll
NgcCtnrSvc -> %SystemRoot%\System32\NgcCtnrSvc.dll
NgcSvc -> %SystemRoot%\system32\ngcsvc.dll
NlaSvc -> %SystemRoot%\System32\nlasvc.dll
nsi -> %systemroot%\system32\nsisvc.dll
OneSyncSvc -> %SystemRoot%\System32\APHostService.dll
p2pimsvc -> %SystemRoot%\system32\pnrpsvc.dll
p2psvc -> %SystemRoot%\system32\p2psvc.dll
PcaSvc -> %SystemRoot%\System32\pcasvc.dll
PimIndexMaintenanceSvc -> %SystemRoot%\System32\PimIndexMaintenance.dll
pla -> %systemroot%\system32\pla.dll
PlugPlay -> %SystemRoot%\system32\umpnpmgr.dll
PNRPAutoReg -> %SystemRoot%\system32\pnrpauto.dll
PNRPsvc -> %SystemRoot%\system32\pnrpsvc.dll
PolicyAgent -> %SystemRoot%\System32\ipsecsvc.dll
Power -> %SystemRoot%\system32\umpo.dll
ProfSvc -> %systemroot%\system32\profsvc.dll
QWAVE -> %windir%\system32\qwave.dll
RasAuto -> %SystemRoot%\System32\rasauto.dll
RasMan -> %SystemRoot%\System32\rasmans.dll
RemoteAccess -> %SystemRoot%\System32\mprdim.dll
RemoteRegistry -> %SystemRoot%\system32\regsvc.dll
RetailDemo -> %SystemRoot%\system32\RDXService.dll
RpcEptMapper -> %SystemRoot%\System32\RpcEpMap.dll
RpcSs -> %SystemRoot%\system32\rpcss.dll
SCardSvr -> %SystemRoot%\System32\SCardSvr.dll
ScDeviceEnum -> %SystemRoot%\System32\ScDeviceEnum.dll
Schedule -> %systemroot%\system32\schedsvc.dll
SCPolicySvc -> %SystemRoot%\System32\certprop.dll
SDRSVC -> %Systemroot%\System32\SDRSVC.dll
```

```
                          SYSTEM OUTPUT.txt
seclogon -> %windir%\system32\seclogon.dll
SENS -> %SystemRoot%\System32\sens.dll
SensorService -> %SystemRoot%\system32\SensorService.dll
SessionEnv -> %SystemRoot%\system32\sessenv.dll
SharedAccess -> %SystemRoot%\System32\ipnathlp.dll
ShellHWDetection -> %SystemRoot%\System32\shsvcs.dll
smphost -> %Systemroot%\System32\smphost.dll
SmsRouter -> %SystemRoot%\system32\SmsRouterSvc.dll
SSDPSRV -> %SystemRoot%\System32\ssdpsrv.dll
SstpSvc -> %SystemRoot%\system32\sstpsvc.dll
StateRepository -> %SystemRoot%\system32\windows.staterepository.dll
StorSvc -> %SystemRoot%\system32\storsvc.dll
svsvc -> %SystemRoot%\system32\svsvc.dll
swprv -> %Systemroot%\System32\swprv.dll
SysMain -> %systemroot%\system32\sysmain.dll
SystemEventsBroker -> %SystemRoot%\System32\SystemEventsBrokerServer.dll
TapiSrv -> %SystemRoot%\System32\tapisrv.dll
TermService -> %SystemRoot%\System32\termsrv.dll
Themes -> %SystemRoot%\system32\themeservice.dll
tiledatamodelsvc -> %SystemRoot%\system32\tileobjserver.dll
TimeBroker -> %SystemRoot%\System32\TimeBrokerServer.dll
TrkWks -> %SystemRoot%\System32\trkwks.dll
UnistoreSvc -> %SystemRoot%\System32\unistore.dll
upnphost -> %SystemRoot%\System32\upnphost.dll
UserDataSvc -> %SystemRoot%\System32\userdataservice.dll
UserManager -> %SystemRoot%\System32\usermgr.dll
UsoSvc -> %systemroot%\system32\usocore.dll
VaultSvc -> C:\Windows\System32\vaultsvc.dll
vmicguestinterface -> %SystemRoot%\System32\ICSvc.dll
vmicheartbeat -> %SystemRoot%\System32\ICSvc.dll
vmickvpexchange -> %SystemRoot%\System32\ICSvc.dll
vmicrdv -> %SystemRoot%\System32\ICSvc.dll
vmicshutdown -> %SystemRoot%\System32\ICSvc.dll
vmictimesync -> %SystemRoot%\System32\ICSvc.dll
vmicvmsession -> %SystemRoot%\System32\ICSvc.dll
vmicvss -> %SystemRoot%\System32\ICSvc.dll
W32Time -> %systemroot%\system32\w32time.dll
WalletService -> %SystemRoot%\system32\WalletService.dll
WbioSrvc -> %SystemRoot%\System32\wbiosrvc.dll
Wcmsvc -> %SystemRoot%\System32\wcmsvc.dll
wcncsvc -> %SystemRoot%\System32\wcncsvc.dll
WcsPlugInService -> %SystemRoot%\System32\WcsPlugInService.dll
WdiServiceHost -> %SystemRoot%\system32\wdi.dll
WdiSystemHost -> %SystemRoot%\system32\wdi.dll
WebClient -> %SystemRoot%\System32\webclnt.dll
Wecsvc -> %SystemRoot%\system32\wecsvc.dll
WEPHOSTSVC -> %systemroot%\system32\wephostsvc.dll
wercplsupport -> %SystemRoot%\System32\wercplsupport.dll
WerSvc -> %SystemRoot%\System32\WerSvc.dll
WiaRpc -> %SystemRoot%\System32\wiarpc.dll
WinHttpAutoProxySvc -> %SystemRoot%\system32\winhttp.dll
Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll
WinRM -> %SystemRoot%\system32\WsmSvc.dll
wlidsvc -> %SystemRoot%\system32\wlidsvc.dll
workfolderssvc -> %systemroot%\system32\workfolderssvc.dll
WPDBusEnum -> %SystemRoot%\system32\wpdbusenum.dll
WpnService -> %SystemRoot%\system32\WpnService.dll
wscsvc -> %SystemRoot%\System32\wscsvc.dll
WSService -> %SystemRoot%\System32\WSService.dll
wudfsvc -> %SystemRoot%\System32\WUDFSvc.dll
WwanSvc -> %SystemRoot%\System32\wwansvc.dll
XblAuthManager -> %SystemRoot%\System32\XblAuthManager.dll
XblGameSave -> %SystemRoot%\System32\XblGameSave.dll
                             Page 188
```

SYSTEM OUTPUT.txt
XboxNetApiSvc -> %SystemRoot%\system32\XboxNetApiSvc.dll

----------------------------------------
ControlSet001\Control\Terminal Server
LastWrite Time Thu Apr 21 04:41:03 2016 (UTC)

Reference: http://support.microsoft.com/kb/243215

  ProductVersion = 5.1

  fDenyTSConnections = 1
  1 = connections denied


  TSUserEnabled = 0
  1 = All users logging in are automatically part of the
  built-in Terminal Server User group. 0 = No one is a
  member of the built-in group.
  Ref: http://support.microsoft.com/kb/238965

AutoStart Locations
Wds\rdpwd key
  StartupPrograms: rdpclip
Analysis Tip: This value usually contains 'rdpclip'; any additional entries
should be investigated.

WinStations\RDP-Tcp key
  InitialProgram: {blank}
Analysis Tip: Maybe be empty; appears as '{blank}'

WinStations\RDP-Tcp key
  UserAuthentication: 1
Analysis Tip: If the UserAuthentication value is 0, the system may be
susceptible to a priv escalation exploitation via Sticky Keys.  See:
http://www.room362.com/blog/2012/5/25/sticky-keys-and-utilman-against-nla.html
----------------------------------------
timezone v.20130830
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Tue Mar 22 13:03:57 2016 (UTC)
  DaylightName    -> @tzres.dll,-111
  StandardName    -> @tzres.dll,-112
  Bias            -> 300 (5 hours)
  ActiveTimeBias -> 240 (4 hours)
----------------------------------------
usb v.20141111
(System) Get USB key info

USBStor
ControlSet001\Enum\USB

ROOT_HUB30 [Thu Aug 13 21:55:44 2015]
  S/N: 4&3a6d4b5b&0&0 [Thu Apr 21 03:18:55 2016]
  Device Parameters LastWrite: [Thu Aug 13 22:02:09 2015]
  Properties LastWrite      : [Thu Aug 13 22:02:57 2015]
    ParentIdPrefix: 5&efed2b0&0

VID_0489&PID_E078 [Fri Sep 11 09:40:59 2015]
  S/N: 6&7bda045&0&1 [Thu Apr 21 03:18:57 2016]
                    Page 189

```
                         SYSTEM OUTPUT.txt
    Device Parameters LastWrite: [Sat Apr  2 16:25:24 2016]
    Properties LastWrite      : [Tue Mar 22 13:08:44 2016]
       ParentIdPrefix: 7&17491d69&0

VID_04CA&PID_300B [Thu Aug 13 22:24:53 2015]
    S/N: 6&7bda045&0&1 [Fri Aug 14 02:00:10 2015]
    Device Parameters LastWrite: [Thu Aug 13 22:54:15 2015]
    Properties LastWrite      : [Thu Aug 13 22:24:54 2015]
       ParentIdPrefix: 7&687b5c8&3

VID_04F2&PID_B47F [Thu Aug 13 21:54:39 2015]
    S/N: 0x0001 [Thu Apr 21 03:18:56 2016]
    Device Parameters LastWrite: [Thu Aug 13 21:54:44 2015]
    Properties LastWrite      : [Thu Aug 13 22:02:57 2015]
       ParentIdPrefix: 6&299b800&0

VID_04F2&PID_B47F&MI_00 [Thu Aug 13 21:54:39 2015]
    S/N: 6&299b800&0&0000 [Thu Apr 21 03:18:56 2016]
    Device Parameters LastWrite: [Thu Aug 13 22:40:18 2015]
    Properties LastWrite      : [Thu Aug 13 22:02:57 2015]
       FriendlyName    : VGA webcam

Vid_04f3&Pid_9999&MI_00 [Thu Aug 13 22:28:13 2015]
    S/N: 5&1d43e48e&0&12345 [Thu Aug 13 22:28:13 2015]
    Device Parameters LastWrite: [Thu Aug 13 22:28:13 2015]
    Properties LastWrite      : [Thu Aug 13 22:28:13 2015]
       ParentIdPrefix: 6&97260fe&0

VID_04F9&PID_02B0 [Wed Mar 23 09:31:33 2016]
    S/N: U63481G5J873107 [Wed Mar 23 09:59:59 2016]
    Device Parameters LastWrite: [Wed Mar 23 09:31:34 2016]
    Properties LastWrite      : [Wed Mar 23 09:31:40 2016]
       ParentIdPrefix: 7&13a85fb5&0

VID_04F9&PID_02B0&MI_00 [Wed Mar 23 09:31:34 2016]
    S/N: 7&13a85fb5&0&0000 [Wed Mar 23 09:59:59 2016]
    Device Parameters LastWrite: [Wed Mar 23 09:31:34 2016]
    Properties LastWrite      : [Wed Mar 23 09:31:40 2016]
       ParentIdPrefix: 8&3a63e2ec&0

VID_04F9&PID_02B0&MI_01 [Wed Mar 23 09:31:34 2016]
    S/N: 7&13a85fb5&0&0001 [Wed Mar 23 09:59:59 2016]
    Device Parameters LastWrite: [Wed Mar 23 09:31:44 2016]
    Properties LastWrite      : [Wed Mar 23 09:31:44 2016]

VID_04F9&PID_02B0&MI_02 [Wed Mar 23 09:31:34 2016]
    S/N: 7&13a85fb5&0&0002 [Wed Mar 23 09:59:59 2016]
    Device Parameters LastWrite: [Wed Mar 23 09:31:35 2016]
    Properties LastWrite      : [Wed Mar 23 09:31:40 2016]
       FriendlyName    : Brother MFC-9340CDW Remote Setup Port (COM3)

VID_05E3&PID_0608 [Thu Aug 13 21:54:39 2015]
    S/N: 5&efed2b0&0&3 [Thu Apr 21 03:18:56 2016]
    Device Parameters LastWrite: [Thu Aug 13 22:02:09 2015]
    Properties LastWrite      : [Thu Aug 13 22:02:57 2015]
       ParentIdPrefix: 6&7bda045&0

VID_0BDA&PID_0129 [Thu Aug 13 21:54:41 2015]
    S/N: 20100201396000000 [Thu Apr 21 03:18:57 2016]
    Device Parameters LastWrite: [Thu Aug 13 22:29:04 2015]
    Properties LastWrite      : [Thu Aug 13 22:28:53 2015]

VID_8564&PID_1000 [Fri Sep 11 09:40:58 2015]
                         Page 190
```

```
                              SYSTEM OUTPUT.txt
S/N: 05NEOR7OF6IS3C1M [Fri Sep 11 09:44:53 2015]
Device Parameters LastWrite: [Fri Sep 11 09:40:58 2015]
Properties LastWrite      : [Fri Sep 11 09:40:58 2015]
S/N: 124BWY3VPN6FOX4C [Fri Aug 14 02:00:11 2015]
Device Parameters LastWrite: [Fri Aug 14 02:00:10 2015]
Properties LastWrite      : [Fri Aug 14 02:00:09 2015]


----------------------------------------
usbdevices v.20140416
(System) Parses Enum\USB key for USB & WPD devices

VID_8564&PID_1000
LastWrite: Fri Sep 11 09:40:58 2015
   SN     : 05NEOR7OF6IS3C1M
   LastWrite: Fri Sep 11 09:44:53 2015

VID_8564&PID_1000
LastWrite: Fri Sep 11 09:40:58 2015
   SN     : 124BWY3VPN6FOX4C
   LastWrite: Fri Aug 14 02:00:11 2015


----------------------------------------
usbstor v.20141111
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100 [Fri Sep 11 09:40:58 2015]
   S/N: 05NEOR7OF6IS3C1M&0 [Fri Sep 11 09:41:03 2015]
   Device Parameters LastWrite: [Fri Sep 11 09:40:59 2015]
   Properties LastWrite      : [Fri Sep 11 09:40:58 2015]
     FriendlyName    : JetFlash Transcend 64GB USB Device
   S/N: 124BWY3VPN6FOX4C&0 [Fri Aug 14 02:00:11 2015]
   Device Parameters LastWrite: [Fri Aug 14 02:00:11 2015]
   Properties LastWrite      : [Fri Aug 14 02:00:11 2015]
     FriendlyName    : JetFlash Transcend 64GB USB Device


----------------------------------------
LAPTOP-D9R76KLQ,Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,05NEOR7OF6IS3C1M&0,14
41964463,JetFlash Transcend 64GB USB Device
LAPTOP-D9R76KLQ,Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,124BWY3VPN6FOX4C&0,14
39517611,JetFlash Transcend 64GB USB Device
----------------------------------------
Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,Fri Sep 11 09:40:58
2015,05NEOR7OF6IS3C1M&0,Fri Sep 11 09:41:03 2015,JetFlash Transcend 64GB USB Device,
Disk&Ven_JetFlash&Prod_Transcend_64GB&Rev_1100,Fri Sep 11 09:40:58
2015,124BWY3VPN6FOX4C&0,Fri Aug 14 02:00:11 2015,JetFlash Transcend 64GB USB Device,
----------------------------------------
xpedition v.20120722
(System) Queries System hive for XP Edition info

xpedition v.20120722
----------------------------------------
wpdbusenum v.20141111
(System) Get WpdBusEnumRoot subkey info

ControlSet001\Enum\WpdBusEnumRoot not found.
ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
----------------------------------------
ALERT: user_run: odd char in path: "C:\Program Files (x86)\Acer\Acer
Portal\AcerPortal.exe" startup
```

Page 191

SYSTEM OUTPUT.txt

ALERT: cmd_shell: Classes\htafile\shell\open\command warning:
C:\Windows\SysWOW64\mshta.exe "%1"
{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}%U{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} %*
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe
Alert: svc: BrYNSvc has a WOW64 value: 1
Alert: svc: CCDMonitorService has a WOW64 value: 1
Alert: svc: Dashlane Upgrade Service has a WOW64 value: 1
Alert: svc: ESProtectionDriver has a WOW64 value: 1
Alert: svc: GamesAppIntegrationService has a WOW64 value: 1
Alert: svc: GamesAppService has a WOW64 value: 1
Alert: svc: ICCS has a WOW64 value: 1
Alert: svc: MbaeSvc has a WOW64 value: 1
Alert: svc: MBAMProtector has a WOW64 value: 1
Alert: svc: MBAMScheduler has a WOW64 value: 1
Alert: svc: MBAMService has a WOW64 value: 1
Alert: svc: MBAMSwissArmy has a WOW64 value: 1
Alert: svc: MBAMWebAccessControl has a WOW64 value: 1
Alert: svc: McNaiAnn has a WOW64 value: 1
Alert: svc: McODS has a WOW64 value: 1
Alert: svc: mcpltsvc has a WOW64 value: 1
Alert: svc: McProxy has a WOW64 value: 1
Alert: svc: mfesapsn has a WOW64 value: 1
Alert: svc: MozillaMaintenance has a WOW64 value: 1
Alert: svc: PEFService has a WOW64 value: 1
Alert: svc: PerfHost has a WOW64 value: 1
Alert: svc: SecureLine has a WOW64 value: 1
Alert: svc: YahooAUService has a WOW64 value: 1
ALERT: svcdll: wbem found in path: winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll

Page 192